

Risk management in cyberspace

James Backhouse¹ with Ayse Bener², Narisa Chauvidul¹, Frederick Wamala¹ and Robert Willison³
**London School of Economics and Politics¹, Bosphorous University²,
Copenhagen Business School³**

While the Office of Science and Technology commissioned this review, the views are those of the authors, are independent of Government and do not constitute Government policy.

1 INTRODUCTION

This paper addresses the social aspects of the information systems security and risk agenda. It counterposes the prevailing focus on technical issues by reviewing research undertaken using a social science perspective. Underpinning this account is a belief that information systems are essentially social systems that rely on an important technical component, and that security is likewise dependent on social behaviour. End-users who are appropriately trained and predisposed towards securing information offer a direct solution to a great many security problems; on the other hand, systems that fail to take account of end-users and their behaviour inevitably contribute to the creation of more vulnerabilities.

It might be natural to assume that a focus on social risks associated with electronic delivery of products and services is an established reality. On the contrary, the prevailing concern is over technical, not social, risks. This paper seeks to draw attention to the behavioural issues that surround the deployment of information and communication technology (ICT) in organizations and an assessment of the present risks and the viability of countermeasures, if they are appropriately managed. The notion of cyberspace does not now smack of its former connotations associated with hacking or with terrorism. Today it refers to interconnected networks or the space within which electronic communications take place and it has become interchangeable and merged with the Internet and World Wide Web (Skibell 2002). This merged notion is adopted for the purposes of this paper.

Security managers address information systems issues from three aspects: technical, formal and informal. The formal element contains the rules and policy that govern the functioning of the information system (IS) and the informal element connotes actual practice and behaviour. Simply focusing on technical problems and solutions can miss the point about how end-users actually form part of the system and how their contributions can spell success or failure – for instance, security can be threatened if users share passwords or choose easily guessed examples. The fruits of risk management activities are embodied in the formalities of a security policy, essentially a set of rules; while the informal system needs to be addressed by means of awareness campaigns and education of users about the importance of security. A culture of security means that end-users, and maybe customers, take on the responsibility themselves for monitoring risk and taking appropriate action. We need to understand more about the interplay of technology, security and risk in the context of cyber operations.

Information security professionals use risk analysis to justify the cost of designing and implementing security on IS. Courtney (1977) and Fitzgerald (1978) were among the first to develop risk analysis methods and by the 1980s, the US Government had adopted risk analysis as a standard for security mechanism design. Courtney (1977) defined risk as the 'product of probability of an exposure occurring a given number of times per year (P) and the cost (or loss) (C) attributed to such exposure'. Therefore, risk (R) is $R = P \times C$. In this insurance-based approach there is an assumption that appropriate statistics are available to perform the calculation. In a social science approach where cultural perceptions are critical, it may be that before counting individual examples there is a great deal of work to be done to agree on the nature of the exposure and what constitutes a risk event in the first place. As the information society cuts through time and space to gather ever more actors in its embrace, the question of the social and cultural basis of information and risk urgently needs addressing. An analysis of the dialectic of theory and practice

in information security can be helpful in avoiding the one-sidedness of basing policy on abstract theories about risks in cyberspace and the rejection of the lessons from theory by practitioners.

This paper draws on organizational studies performed between 1998 and 2004 into the behavioural and organizational aspects of risk and security in the context of global companies whose use of web-based technology is critical to both their front and back offices. Each study focuses on different aspects of security and risk in information systems and adopts a different perspective for the purpose. Undertaken in a global bank, the first study demonstrates how, despite a collective aim to deliver a new Internet banking product, different perceptions of risk and security flourished within the same project team. Insights emerge into how the various actors construct the trustworthiness that lends credibility to communications and the role of the medium chosen. A second study explores the role of criminal opportunity as a concept for analyzing IS security situations, taking the perpetrator's context as a rogue insider as the analytical focus. A third study focuses on internal control issues in the context of a geographically dispersed corporation and shows how cultural issues can drastically affect the expectations–reality equation of control exercised from a distant western headquarters. As back-office financial sector work is shifted towards developing countries, the risk and security implications are highlighted. The fourth study compares how Public Key Infrastructure (PKI) was introduced in an oil company and a global bank and recounts the critical role of institutional factors in determining the success of the deployment. There are important implications for all enterprises seeking to create secure interoperability internally or externally. A discussion follows in Section 6 on the lessons to be drawn from the review of the cases.

Using a social science approach to security permits the adoption of a range of perspectives, rooted in different theories and frameworks and in their respective disciplines. For understanding and managing the technical aspects of information security, an engineering and computer science background remains essential, but for dealing with the pragmatic and semantic aspects of information security, other forms of preparation are required which can offer legal, political, sociological and economic insights.

Our general aim is to demonstrate that IS security and risk research must go beyond the usual prescriptive and technical advice where IS security is seen as a purely technical concern (Wood 1995; Parker 1997; Osborne 1998; von Solms 2001). Since information systems are viewed here as more than merely technical systems, this body of research is able to address that part of the security risk agenda that might formerly have been dismissed as a troublesome 'people problem' and hence not of prime concern.

2 RISK PERCEPTION AND COMMUNICATION

At the core of risk management in any social or organizational context lies the issue of how social actors discern risks and enter into communication about them and how they may be addressed. In this first case study Bener (2000) researched risk in a project that aimed to launch an Internet banking product in a top-tier global bank (NIMETBANK in her study) and provided interesting findings directly relevant to risk perception, risk communication and trust and credibility. A field study and a supporting customer survey confirmed that individuals and institutions processed messages they received and developed their perceptions of these messages according to their previous experiences, the social and economic climate, their cultural backgrounds and the trust they placed in the messages and their sources.

The stakeholders in the project management team included representatives from three broad categories in relation to the Internet banking product within the global bank – the UK Business and the Bank Information Security Office (Users), the US-based Advanced Technologies Group (Supplier), and the information technology infrastructure, operations risk, corporate audit, project risk review, teams, etc. (Support).

2.1 Stakeholders Defined and Perceived Risk Events Differently

The priorities of the stakeholder groups reflected their cultural backgrounds as described by Douglas (1985). They were largely influenced by the organizational structure and the findings confirmed that institutional structure is the ultimate shaper of risk perception. Each unit in the project at NIMETBANK brought its own view of risk and organizational imperatives clearly shaped

by their attitudes and beliefs. Risks were overlooked if they conflicted with the goals of the stakeholders. Since stakeholders had different priorities, they also attenuated or intensified certain aspects of risks according to their own priorities.

For example, the goal of the UK business unit was to have more functionality in their product in order to be ahead of their competitors, and saw no security risk in delivering on the Internet. By contrast, the bank Information Security Officer thought, unsurprisingly, that security on the Internet was the biggest problem. He doubted that the risk could be covered even by security measures, but that if a customer lost money because of a security breach, the terms and conditions should protect the bank against claims by the customers: "Hackers are always ahead of the others and therefore it is difficult to protect the bank from them. Therefore, my main objective is to draft the terms and conditions properly and tight enough to protect the bank from suing customers" (Bener 2000, p. 151).

In all, six major risk events were discussed among members of the project team and they crystallize the divisions and differences among the units on the perception of risks.

Personal Identification Number (PIN): In view of the security concern perceived by an audit team member: "Security is the single most important thing to look for in the Internet banking project. Customers will be able to transfer money all over the place and if they can access their bank account from their homes, anyone else can" (Bener p. 149).

The audit team suggested a 6-digit rather than 4-digit PIN, a proposal eventually overruled on the grounds of lack of conformity with competitors' banking products.

Private Dial-up Network: The Advanced Technologies Group (ATG) suggested that if the security of the Internet was an issue a private dial-up network could be established for the customers of NIMETBANK. The idea was supported by the technology infrastructure group and others. However, after lengthy arguments between the business units and the information security office, the UK marketing director explained:

when we had to make a decision to go on the Internet we consulted ATG. They gave us pros and cons of both options honestly. In regards to the Internet they did ring the alarm bells, therefore we decided against the dial-up since its cost did not justify its benefits (Bener p. 167).

Delivery Time: UK business saw time to market as critical for them: "The only risk in this project I could imagine is the time for delivery. Getting it up and running and the web site. Just the risk of the schedule" (Bener p. 154).

Operational Risk: UK operations had to incorporate some of the new features of the product into their host system. They also had to prepare for the expected increase in customer volume and, hence, an increase in transaction volumes. For them, "the riskiest factor has always been, besides time and quality, that not everyone does things in the same way in the technology department" (Bener p. 156).

Additional Product Feature: The current Internet banking product did not allow for a prospective customer to open an account with the bank in an online manner. UK business thought that online account opening was a critical competitive advantage as well as a significant cost saving for the operations. However, ATG declined to modify the existing product on the grounds that it did not have a secure solution to implement this change in the given time frame.

Co-brand Agreement: UK business aimed at acquiring new customers with the Internet banking product, and entered into an agreement with a local Internet Service Provider (ISP) to offer free Internet access to its customers. However, the technology infrastructure team raised a concern on the grounds that this was a major breach of security as far as the information security policies of the bank were concerned. The European audit manager explained: "we also sent a memo that the business units could not enter into marketing arrangements with local ISPs in their respective countries since the ISPs could tap into the bank's backbone and this would be a major security breach" (Bener p. 152).

2.2 Importance of the Social Climate on Risk Perception

The prevailing social climate (of the late 1990s) had a positive impact on the stakeholders of the

project team and the customers of the NIMETBANK towards Internet usage. Stakeholders based their decisions on consideration of the social issues beyond those internal to the bank. Key issues here were the stiff competition from other well-known UK banks who were bringing Internet banking to millions of customers and the growth in popularity of the Internet for financial and commercial transactions. A third issue was the increasing publicity being given by the media to incidents concerning Internet and information systems security, raising the stakes for Internet ventures of this kind. All three issues played a part in shaping perceptions of risk.

2.3 Trust Established through Competence

Openness and objectivity in the risk communication on its own was not enough to establish trust between the parties. Trust was only established through the competence of the source or transmitter in the message process. Several findings confirmed that as long as the transmitter was competent, the receivers paid less attention to the source of the message, and vice versa. Another conclusion was that the personality of the communicator, with attributes of ability and integrity, was also important in establishing trust. Trust was seen to be placed in those who had delivered in the past. Those units associated with the delivery of technology were well regarded and trusted. A UK business manager explained her trust in the ATG:

I trust ATG very much. They were very successful lately in the implementation of the PC banking product. Not only that, ATG has been successful all around the World. They manufactured and installed all of the more than 3,000 NIMETBANK automated teller machines in many countries, including the UK. My experience has always been very good when working with them. I am sure they will be successful in implementing the Internet banking product here (Bener p. 165).

By contrast, where there were doubts, they were driven by organizational rivalries, for example, the UK marketing director recounted that:

we just ignored what they [technology infrastructure] said since they could not explain why we were at risk, and then, we started thinking that the reason they were pushing so hard was to get us on the global ISP contract they signed last year so that they could take the whole credit (Bener p. 167).

2.4 Risk Communication

The matter of how to communicate risk issues has been a vital concern for business and government alike, whether it relates to cyber risks or more traditional risks.

Risk Communication is an interactive process of exchange of information and opinion among individuals, groups and institutions. It involves multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions and reactions to risk messages or to legal and institutional arrangements for risk management (National Research Council 1989, p. 21).

Researchers such as Fesseden-Raden et al. (1987) and Krinsky and Plough (1988) have taken this definition further, so that risk communication consists not only in the exchange of information among the parties involved, but also in the wider institutional and cultural contexts within which risk messages are articulated, transmuted and embedded. Risk communication represents a 'tangled web' of messages, signs and symbols. Besides the intended risk message, other unintended messages may be transmitted through signs and symbols and, hence, result in outcomes that are unpredictable. Moreover, because most hazards have a history, this too influences the receivers' interpretations of the messages.

The basic communication model describes three roles in the process: sources of a message, transmitters of a message, and receivers of a message. Interactions about risk issues may serve to amplify or attenuate communication signals. Social amplification of risk suggests that during the communication among stakeholders, whichever role they make take, source or transmitter, the communication process either intensifies or attenuates certain aspects of risk because of cultural factors.

Generally, because of distance, communication between members of the teams took place through email or telephone. However, inter-team communication was usually face-to-face at scheduled or informal meetings. The interviews for this study revealed that email was a very dominant communication medium for NIMETBANK employees. It was observed that, even among the members of a team who were located in the same building, email was used very frequently with

reasons cited such as,

information can be disseminated to many receivers in a more efficient way

communication gets recorded and senders and receivers do not forget what was said,

it's easier to remember what you've said; what you've asked [others] to do, what they've promised or undertaken to do for you and what they've done (Bener 2000 p. 151).

There were conflicting messages received from the employees interviewed about the effectiveness of methods of communication within NIMETBANK. Most employees said that face-to-face communication was best, but because of time constraints, email, telephone and teleconferencing were used the most. Almost all the employees affirmed that sometimes more emails than necessary were generated. One employee from ATG said, "Its got to be a mix between email, telephone, teleconferencing and face-to-face communication; coming up with the right mix is very difficult. If you have the wrong mix, you can waste a lot of time, not get the job done. I don't know what the right mix is" (Bener p. 158).

The credibility of communicators is critically dependent upon the trust placed in them. In other words, in order for us to trust the message, we need first to trust the communicator of that message. Credibility of information sources is a key factor in risk communication such that credible sources are those that shape risk and security policies within the organization.

In summary, the findings of the study are as follows:

- risk perception: different stakeholders hold different perceptions about what risks exist and this has implications for risk management;
- trust and credibility: trust is given to those who have 'delivered' in the past; and
- risk communication: trusted sources are critical in risk communication, amplification and attenuation are endemic, and email is the dominant medium.

While none is surprising, the importance for risk management is not to overlook them. Risk perception, communication and trust all nestle in the bosom of socially constructed information systems that must be constantly reinterpreted if security is to be achieved.

3 OPPORTUNITY – PERCEIVING CYBER CRIME AND SECURITY

This section focuses on the concept of criminal opportunity and information security based on a case study by Willison and Backhouse (2003). More precisely, it questions the nature of this phenomenon with regard to the organizational context and the considerable threat posed by dishonest staff. One alternative approach to help mitigate the risks associated with rogue employees is to reduce their opportunities for computer abuse. To this end, a model to help understand the relationship between such staff, their environment and opportunity is advanced. In the literature that directly addresses the issue of opportunity, the focus divides into two distinct areas: opportunity as both a motivator of criminals and as an outcome of deficient security.

A few writers have discussed opportunity in terms of the motivational impact it may have on individuals (BloomBecker 1984; Forester and Morrison 1994; Hitchings 1995). In an early paper on the issue, for example, BloomBecker cites eight types of motivational factors. One of these is 'the land of opportunity', where rogue employees exploit security loopholes spotted during the course of their daily work activities. However, other writers who discuss the relationship between opportunity and motivation merely mention this phenomenon in passing: "Experts on computer fraud attest to the fact that opportunity more than anything else seems to generate this kind of behaviour" (Forester and Morrison 1994, p. 41).

With the aim of raising practitioners' awareness, the UK Audit Commission has been eager to spread the message regarding the relationship between poor security and opportunity. Its report, *Opportunity Makes a Thief* (Audit Commission 1994), indicates that one of the primary reasons for 'computer abuse' is a disregard for basic controls. More precisely, this disregard manifests itself in a failure to implement and maintain such controls. These findings are mirrored in the Commission's next report *Ghost in the Machine* (Audit Commission 1997), which finds 'little improvement' with regard to the provision of internal controls. Furthermore, this intransigence is reflected in the 2001 report which states: "Auditors and security specialists continue to stress the need for proper control and security measures. Nevertheless, the majority of breaches of IT security are still caused by a

lack of the basic fundamental controls and safeguards” (Audit Commission 2001, p. 17).

This view is supported by other writers in the field who have additionally and explicitly pointed to how poorly implemented and enforced controls might engender opportunities (Bologna 1993; Comer 1998; Stevenson 2000). Indeed, both Comer and Bologna stress how opportunities form one of the two key elements – the other being motivational factors – that must be addressed when combating computer fraud in organizations. But what exactly are the factors that lead to the absence and poor maintenance of safeguards?

3.1 Complacency

Complacency about IS security is a primary reason for the absence of the appropriate safeguards (Audit Commission 1997; Hinde 2001). As noted, this manifests itself in the failure of some organizations to implement even the most basic controls, leaving their systems vulnerable and possibly forming the conditions that create opportunities. The three UK Audit Commission reports cited above clearly demonstrate this. A key control, for example, is a security policy (Dorey 1994; Backhouse 1997; Osborne 1998; Nosworthy 2000). In 1994 and 1998 the Commission reports indicated that of the 1,073 and 900 organizations surveyed, one-third failed to implement this safeguard. While this position had improved by 2001, one-quarter of the 688 organizations still had failed to pay heed to the alarm bells.

3.2 Failure of Focus

While companies may fail to appreciate the value of information security, they may also fail to recognize potential threats (Parker 1997; Hinde 2001; Riem 2001; Wright 2001; Yapp 2001). A 2002 global security report reveals in a survey of 459 organizations:

Yet again we see greater concern about vulnerability to external attack (57%), than internal (41%), and yet leading research groups continue to confirm that more than three quarters of attacks originate from within organisations ... an alarming amount of evidence remains that organisations are lacking fundamental management information about security breaches (Ernst & Young 2002, pp. 8-9).

This is confirmed by Parker (1997) who argues that the ‘distorted image’ of security held by top-level business people is often ‘informed’ by trade publications such as the *Wall Street Journal* and *Forbes*, whose focus is more on the newsworthy than on the mundane. Additionally, the distorted image of security held by managers is often related to a myopic understanding of the problem area and how it should be addressed. Several writers have confirmed that in many organizations IS security is often perceived as a purely technical concern (Wood 1995; Parker 1997; Osborne 1998; von Solms 2001). The downside of this perspective is that it fails to encompass the whole of the problem domain and, hence, fails fully to appreciate all the components that constitute an information system with its technical, formal and informal elements.

3.3 Interrelated Controls

One problem often overlooked when safeguards are introduced is their interrelated nature. Security is very much like a house of cards: inadequate consideration for one area will impact on another, possibly creating conditions that help form an opportunity. One safeguard, for example, is an information security policy. The 2001 Audit Commission report revealed that 25 per cent of the 688 surveyed organizations still had no security policy. Through the creation and maintenance of a security policy, management can provide support and direction for information security in an organization. There is no denying the importance of a security policy as a cornerstone in the development of an organization’s control environment (Dorey 1994; Backhouse 1997; Osborne 1998; Nosworthy 2000). However, unless the policy is brought to life through education and awareness programmes, then all the work undertaken to create a policy will ultimately have been a waste of time (Spurling 1995; Thomson and von Solms 1998; Nosworthy 2000).

3.4 Implementation of Inappropriate Controls

Even prudent companies that wish to establish effective security across the board, may unwittingly create the conditions that help to form opportunities through the implementation of inappropriate

controls (Warman 1993; Olnes 1994; Luzwick 2001). If the introduced safeguards provide a sub-standard level of security then the IS will be left vulnerable. However, the same is also true if the safeguards are perceived by staff as unworkable in the organizational context. One of the perennial problems for IS security is its uneasy relationship with business objectives. Although there is an obvious need to reduce the risks to an IS, the respective countermeasures are often seen by users as a constraint, given the range of tasks required to fulfil the objectives. If the safeguards are perceived to be too heavy-handed or impractical (or both), staff may circumvent the controls just to make their lives easier, or they may even rebel against such controls as in the recent case at British Airways, where security tokens were introduced to monitor staff without adequate canvassing of staff opinion.¹ Again, non-compliant behaviour leaves systems vulnerable, possibly providing opportunities for rogue employees. In this sense, although safeguards are obviously introduced to reduce risks, with a heavy-handed approach, they may in reality create them.

3.5 Implementing Safeguards

Aside from the inappropriate nature of safeguards, a related issue concerns the implementation of controls. Poor implementation can negate improvements in security for which a safeguard was designed. Schneier (1998) discusses cryptographic systems as a case in point. He notes several problems pertaining to the poor implementation of this safeguard. With some systems, the plain text which the user wishes to encrypt is not destroyed after the process takes place. Other systems use temporary files on a computer in case of a system crash. While this is prudent, if these systems are wrongly implemented, the plain text is left on the hard drive. Schneier further notes how some poorly implemented systems can even leave the cryptographic keys on the hard drive.

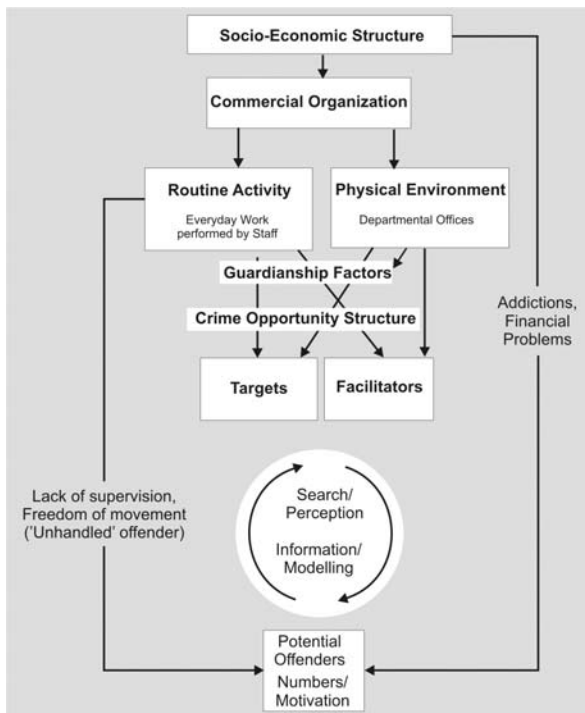
3.6 Compliance Review

A key prerequisite of IS security is the need to confirm on a routine basis that the existing controls are working effectively. One of the messages repeated in several UK Audit Commission (1994, 1997, 2001) reports is that many organizations are failing to check whether their controls are operating as intended. As a consequence those safeguards that are failing to perform are leaving IS vulnerable. Furthermore, these vulnerabilities may persist for considerable periods of time, given the failure of some companies to monitor their controls.

3.7 Opportunity Structure – A Model for Security?

The Crime Specific Opportunity Structure (Clarke 1995), recognizing the threat from dishonest insiders, focuses on the opportunities afforded the potential perpetrator with regard to the organizational context.

Figure 1 Crime specific opportunity structure



The model set out in Figure 1. draws on a number of criminological theories such as Situational Crime Prevention (Clarke 1997), the Rational Choice Perspective (Clarke and Cornish 1985, 1986, 2000), Environmental Criminology (Brantingham and Brantingham 1991), Routine Activity Theory (Hirschi 1969; Felson 1992), and Lifestyle Theory (Hindelang et al. 1978). It attempts to provide a new perspective and fresh insights into this opportunity risk.

This model can support information security work by exploring the constituent elements that, together, may afford an opportunity to the criminal and permits an examination of how safeguards interact to form a coherent control environment. Within the 'Opportunity Structure for Crime', the physical environment affords both *targets* and *facilitators*, for example, easily-guessed passwords or PCs left unattended that facilitate access to valuable transaction data that can be modified to the advantage of the rogue insider. Furthermore, lifestyle and routine activities also influence the number of targets. The behaviours inscribed in lifestyle and routine activities, that is, work, leisure, residence and shopping, can either enhance or hinder guardianship and can supply victims.

At a macro level within the structure, the *socio-economic structure* influences the lifestyle/routine activities and the physical environment. The former includes demography, geography, industrialization, urbanization, welfare/health, education and legal institutions. The socio-economic structure also partly determines the number of potential offenders through sub-cultural influences, such as neglect and lack of love, alienation, etc. (identified by traditional criminology), and partly through lifestyle and routine activities. Classic fraud profiles point to a different set of socio-economic factors that may motivate an offender. These include addictions in their various guises, marital breakdown, financial problems and the like (Bologna 1993). Routine activities and lifestyle can influence the degree of social control afforded by intimate handlers, leading to a possible lack of supervision and freedom of movement. The number of potential offenders is also partly determined by routine activities in terms of the degree of supervision afforded by managers or security-minded peers, leading to either handled or unhandled staff and, hence, to potential offenders. In the normal context there usually will be a capable guardian, possibly a supervisor or a fellow employee, whose presence dampens the ardour of perpetrators to commit their crimes. An interesting issue arises with teleworking where the guardian functions are embraced by an increasingly invasive technical infrastructure.

The opportunity structure addresses the interactions between potential offenders, facilitators, targets and victims. These interactions suggest the nature and scale of the opportunities for crime. Furthermore, the interplay between these entities largely takes place in the 'action' and

subsequently 'awareness' spaces of offenders as indicated by the search/perception – information modelling sections of Figure 1 and as highlighted by environmental criminology. The offender's perceptions – highlighted by the rational choice perspective and also by environmental criminology – of the risks, efforts and rewards associated with such spaces play a crucial role in defining the opportunity structure.

The Crime Specific Opportunity Structure model has been applied to analyze the Barings Bank disaster using the reports supplied by the Bank of England and SIMEX, the Singapore Exchange (Willison 2002). The issues raised by the model of lack of supervision and freedom of movement were reflected accurately in the Leeson affair. From the start of Leeson's career at Barings Futures Singapore there was confusion about who actually managed him: "some members of management believed that responsibility for certain activities rested with other managers, who deny they had such responsibility" (Board of Banking Supervision 1995, para 2.28).

The absence of an 'intimate handler' meant that Leeson was able to undertake the fatal unauthorized trading. Furthermore, the little supervision actually exercised came from managers in Barings, who did not understand the trading of futures and options, for example, James Bax and Ron Baker. Of course where there is an inability to understand the work being supervised, there remains only trust as a support, in the Leeson case, decidedly misplaced – for it is "extremely difficult to impose control systems that are so draconian that people who have the responsibility to act in a trustworthy fashion should nonetheless have people looking over their shoulders on a minute by minute basis, to make sure they don't conceal the evidence of their transactions".²

4 INTERPRETING CONTROL RULES

Another perspective on social risks in a world where ICT is gradually defeating the imperative of distance has been developed by Chauvidul (2003). Using a semiotics framework, in this, the third of the case studies presented here, she examined the relationship between formal systems and informal norms in internal control systems in a global bank. She argued that the global policies and standardized manuals and procedures of multinational firms cannot be internalized and interpreted in the same way in every branch, as anticipated by the management. The risk under scrutiny is the breakdown of control systems in contexts where ICT has enabled a globalized and distributed organization. The main objective was to analyze in-depth the interaction between formal and informal systems. The focus of the study was on the people who played a significant role in the control systems. In pursuing this aim, an interpretive case study of a global bank was conducted in two branches, London and Bangkok. Four themes are of particular interest with regard to risk management in such organizations.

4.1 Organizational Structure

Transnational companies, especially in the finance sector, have increasingly adopted the matrix system of management, eschewing the traditional multi-level hierarchical approach. With pervasive ICT to support decision-making and given the benefits of a 'flatter' control pyramid and devolution of power away from the centre, such a development is not surprising. However, interviews in Thailand revealed discomfiture with the new structure. One implication was that the attitude towards written guidelines was 'don't bother to check it'. Local guidelines were not being updated and were being ignored. As one Western staff member working in Thailand put it: "I think the guidelines are useful as a reference source, but at the end of the day, someone who knows their job won't really need the guidelines. They can think creatively, conceptually and rationally" (Chauvidul 2003, p. 121).

4.2 Control Structure

The loss of the powerful figure of the bank manager and the replacement by a matrix reporting system cut against the grain of the prevailing Thai culture, whereas the organizational impact of the new system in London was minimal. Many Thai staff felt that they no longer had support and back-up from management in their branch. The result was reduced motivation and general low morale. This confirms the findings of researchers who examine transnational companies who argue that managers in such companies should be responsive to individual companies and different cultural contexts (Wasilewski 2002; Bartlett and Goshal 1989). Local factors should be explored when

implementing policies and procedures and internal control systems. Many of the 25 interviewees agreed that under the matrix system, there are more problems of communication and coordination:

There is no one at a high level in the branch who has the final say whether one thing should be done or not because now they rely on communication - who has the best ability to make a better presentation. This is because those who have the final say are not in the Bangkok branch and so they would not know the local environment (Chauvidul 2003, p. 134).

4.3 Globalization and Cultural Context

The 'one size fits all' approach was also demonstrated to be inappropriate in the case of the ABC Bank. One of the biggest challenges for multinationals using ICTs is how to manage global policies with appropriate consideration for the norms of specific cultural contexts (Bartlett and Goshal 1989; McDonald 2000; Thorne and Saunders 2002). The global policies of multinationals usually reflect embedded western values and culture and may not easily be institutionalized in other contexts where personnel have their own deeply held beliefs. Failure to acknowledge the existence and diversity of different cultures can disrupt control systems and, hence, give rise to new 'social' risks. For example, an analysis using a framework from Hofstede (1991) revealed nine separate dimensions of this kind of 'social risk', three of the most interesting in the context of this paper are:

Face Saving – where some staff members feel embarrassed about asking a question or imposing themselves on someone else. The risk here is that employees will not share their new ideas with their boss or colleagues. When they do not understand certain rules, they may make wrong judgements.

Criticism Avoidance – Thai employees like to avoid criticism and confrontation. They do not want to change the way they do things because they do not like to hear negative comments. The risk is that when the bank tries to change or introduce different ways of doing things, this can sometimes lead to low motivation levels and general unhappiness on the part of Thai staff.

Kreng-Jai – Thai employees do not like to say 'I cannot do it'. Honest opinions or straight answers are hard to elicit from Thai staff. Auditors receive an inaccurate picture of the state of play (Chauvidul 2003, pp. 40, 184).

4.4 The Relationship between Formal and Informal Systems

ABC London is a rule-based branch with a culture common to the head office. Here the normal situation is for staff to follow rules and update their guidelines. When ambiguities arise, staff use personal judgment to make the best decision. In some areas there may only be norms rather than rules, and the guidelines or formal systems will be appropriately updated. In the Thai branch the status of the formal rules had been undermined by the organizational changes. Many of the key operating procedures just did not seem to apply in a developing country and, with demotivation winning the day, the formal system became discredited. Staff would resort to personal judgments in the absence of appropriate rules and, in this context, such practices presented increased risk for the bank. One staff member of the Thai back office declared that when she needed to ask about the interpretation of particular rules, because of the matrix system, she had to consult someone from head office in Singapore. However, staff in Singapore complained that she asked too many questions: "... they asked me why I did not use my common sense. Actually I wanted my work to follow the global standard, that's why I asked them. I do not want to use my own interpretation" (Chauvidul 2003, p. 196).

In a broad sense internal control can be considered as a part of IS security, which involves minimizing risk arising from inconsistent and incoherent behaviour of actors with respect to compliance with internal control systems. As ICT facilitates ever larger global networks of organizations, the danger is to assume that the individuals who interact with the technical system all hold the same values and interpret control information in the same manner. Cultural differences will impact increasingly on organizational security as ICT becomes more pervasive. The key

insights from this case study are that

- interpretation of formal rules is mediated into behaviour through local cultures;
- local cultures may clash with head office values and intentions creating insecurity; and
- the 'view from the bridge' may just be a mirage.

5 INTEROPERABILITY IN TWO GLOBAL ORGANIZATIONS

Interoperability is one of the biggest problems facing public and private entities that use the Internet for commerce, business or government – how to assess 'stranger' identities in an 'open' environment where the burning questions are which online identities can be trusted, and how much. Deploying digital certificates and PKI is one way in which identity management has been tackled across the globe. The X.509 standard has been widely promoted as the *de facto* model for underpinning PKI because of its potential for eradicating interoperability problems between 'stranger' infrastructures (Chokhani and Ford 1998). The standard is an offshoot of the grand attempt in the 1980s to create a global directory of named persons and entities under the ITU-X.500 project (Ellison 1997). Nevertheless, the idea of a linked global directory failed because organizations refused to publish the names of their employees in this repository, thus dealing a blow to PKI interoperability. As a result, the search to link up multiple stranger PKIs has been a major preoccupation of the security community for many years. This section presents the fourth case study, which underlines the organizational issues that prevent interoperability as compared to the considerable emphasis that is given to technical standards and protocols.

5.1 PKI to Secure Online Working

Using a power analytical framework drawn from political science (Clegg 1989), research was undertaken in two global companies in the oil and finance sectors (Wamala 2002), Oilcom and Bankrecht, respectively. Oilcom is a large and diverse energy firm and is among the world's biggest oil companies. Oilcom operates in over 135 countries. Bankrecht is one of the world's largest and most influential financial institutions with assets worth over £428 billion and a workforce of over 70,000 working in 1,500 offices.

Once upon a time Oilcom in common with other big companies had a closed network, which was opened selectively under very strict controls. What we now have is an open internal network, which we selectively close One method of selectively closing this network is providing strong authentication, identification, non-repudiation and all these good things which you get from PKI – if you do it properly (Wamala 2002, p. 5).

In the recently merged Bankrecht the reason for the adoption of PKI was very straightforward,

With the PKI our goal was that all communication should be encrypted so that even the so-called administrators cannot see any of the data The law here is that you must be physically in the country to access the data. PKI gives us a way of ensuring that the information is not revealed easily (Wamala 2002, p. 10).

Both these assertions are sound, yet a detailed social and organizational study revealed the underlying risk of failure in the valiant search for security and interoperability.

5.2 Critical Role of Institutional Arrangements

The critical observation that arises from these two cases is that the relative success of Oilcom's PKI as compared to the problems experienced at Bankrecht was due neither to the technical efficacy of the product nor to its cost. The success of PKI in Oilcom appeared to be due to its supporters' engagement in a shrewdly orchestrated campaign to knit it with the existing institutional order. Because of this alignment, PKI has become an accepted part of organizational life at Oilcom without much ceremony. Why was this possible?

Centralizing tendency. Oilcom introduced PKI at a time when there was a drive to achieve more consistency in its global operations. The firm not only drafted policies to support this goal, but also put in place global ICT systems including a Global Desktop (GD) that supported this principle. Among other objectives, GD was aimed at increasing the number of PCs under the control of the central information technology (IT) division from 69 per cent to 100 per cent. Furthermore, when

Oilcom moved to its new Active Directory, it simply replaced another enterprise-wide X.500 directory.

Security token use was established practice - moreover, badges and smart cards had already been institutionalized in the organizational life at Oilcom over the years and building designs assumed their use.

Shrewd systems design. The factor that ultimately clinched the institutionalization of PKI at Oilcom was the smartcard design, which combined physical access, network log on, lunch pass and document-signing capacities. Employees used the card to accomplish many of their everyday organizational tasks.

By contrast, at Bankrecht none of these conditions was in place.

Recent merger not fully digested. Because the company was still in the aftermath of a merger it did not have a widely accepted institutional order. The firm was in the throes of an open culture clash between the two groups of employees.

Weakened IT division. One of the biggest losers in the merged entity was the IT division because it ceded the command of financial resources to the business divisions. The business divisions effectively took over the governance of IT. They chose which projects to pay for and often excluded large infrastructure projects that they suspected would threaten their autonomy. The situation is summarized by a PKI engineer as follows.

I am not aware of any common IT services. ... we don't have an IT team within Bankrecht that tries to enforce common practices within the divisions. ... At the moment, it is the business divisions that have the money to pay for IT projects so centralizing the service will involve moving the money away from them (ibid p. 14).

The common directory problem. The tussle over resources between the business divisions and Bankrecht Head Office negatively affected the take-up of PKI. This is clear in the stalemate over a common directory. One of the reasons for the relative success of PKI at Oilcom was the deployment of a common Active Directory (AD). Bankrecht has been unable to implement a common AD because this was at odds with the autonomous operations of its business divisions. The absence of a common directory was not the only factor impeding efforts by Bankrecht to create a single domain. It also accentuated the proliferation of PKI islands, as one PKI engineer lamented

One of the key things that I think is gonna affect the ability of Bankrecht to function as a group is the failure to deploy group-wide Active Directory. Over the future that will be significant. That failure was basically due to some technical issues within the product, and political issues (Wamala 2002, p. 14).

There are problems in using a centralized directory running an AD solution. The biggest problem is that it assumes a unified, all-powerful and well-financed IT division. However, in many large global organizations, the IT division lacks such power because of the absence of a common account to pay for infrastructure projects. Many organizations such as Bankrecht simply do not have such a division. Perhaps, even more critical is the assumption implicit in AD that organizations have distinct groups of employees that do not overlap. As observed by a PKI engineer, in practice, Bankrecht, in common with other global organizations, has many overlaps between geographical and functional roles.

Bankrecht has six, seven, eight, nine subdivisions? I do not know how many! You see where my problem begins? There are official and non-official subdivisions. How do you classify those? Because what a PKI can allow you to do is by creating groups, you can make people have access only to certain data. If you say everyone is a Bankrecht employee then you do not have that finer granularity that the application offers to have more inbuilt security (Wamala 2002, p.15).

Because the group was still integrating newly acquired businesses in the US and in its home base country, it would take some time for clearly defined groups to emerge. Bankrecht was not ready for interdomain interoperability since it had failed to consolidate its own internal PKI initiatives. The absence of a central IT function in a large organization generally means that problems arise with interoperation because different business divisions are likely to implement different technologies. Even in cases where the same technology has been implemented group-wide, such as at Oilcom, there often are significant modifications to the infrastructure in different parts of the world to

appease dissenters in far-flung divisions and to cut out the more centralizing features of an AD that demands a robust telecommunication infrastructure. These compromises complicate PKI deployment and increase future interoperation costs.

5.3 PKI Islands put Interoperability at Risk

Potentially a more critical risk to Oilcom's future interoperability is the emergence of PKI islands within the outside-facing trust services. Individual business units have continued to spend on external PKI services with serious consequences as observed by a security consultant.

We lack coordination around the external uses of Trust Services. ... That is the worry because we will get to a situation where we will need to be looking into Microsoft, Entrust, Baltimore, Entegriy, RSA technologies and certificate provisions from a whole variety of different providers and we will have to somehow integrate all those into our technical infrastructure. We must understand policy and procedural implications as well because we have to tie our internal processes to these external requirements. Maybe islands of PKI is all we can achieve with external PKI (Wamala 2002, p.17).

The accumulated effect of the absence of a consistent approach is the creation of islands that have to be expensively harmonized in the future. Consequently, Oilcom and Bankrecht were inadvertently moving from interoperable domains to islands representing a combination of sub-domains. These global, heterogeneous and distributed organizations are not using the PKIX³ model with its assumption of a central/root Certification Authority. Instead, they are depending more on the 'circles of trust' approach by participating in closed trade bodies such as Trade-Ranger and Identrus. These bodies are informal in their origins, but are semi-formalized through the use of contractual agreements. The downside of the use of contracts is that organizations become involved in multilateral agreements that grow exponentially because each time a new member is added they have to sign individual agreements with all other existing members. Contracts demand constant changes in processes and policies to accommodate different relationships and, moreover, they tend to nullify the biggest advantage of e-commerce, that is, the conduct of transactions in real time.

In summary, it is clear that:

- PKI technology needs centralized directories and hence power to be successful;
- in the absence of a powerful IT Department, PKI projects may be led by the businesses;
- interoperability is jeopardized by piecemeal approaches necessitated by power conflicts; and
- institutionalization is eased by linking identity tokens with realization of routine behaviours.

6 SOCIAL RISK MANAGEMENT REVIEW

As the information society unfolds more social risks are destined to make themselves felt. Prudent governance of a society predicated on cyber operations will demand that these risks be acknowledged and that at least some of them be attended to.

The following section recapitulates the issues examined in the four case studies and sets out some of the questions that emerged.

Perception and communication. Drawing upon cultural and communication theory, the first study in Section 2 opened up the dimension of risk perception and communication. In the context of the risk society, it is increasingly urgent that more research be undertaken into the criticality of risk perception for both business and social affairs. How are cyber risks conceptualized at both organizational and societal levels? Who are the sources and transmitters of cyber-risk communications? How does the choice of medium influence the perception of cyber risk? For the cyber organization, how can the various stakeholder views be appropriately reconciled and fed into security policies and procedures addressing those risks? Different perceptions can be a source of strength in the analysis phase, but not once policy has been decided. What emerges from the first study is a basis for rejecting the idea of objective risk and for developing a concept of many subjective understandings of risk. The issue for the organization is how to reconcile the different perceptions into an input into a single policy vehicle to deal with contingency and security. A further issue lies in deciding the most effective means of communication of risk, balancing, for example, effective but costly face-to-face models with efficient but impersonal emails. To what extent does the medium impact on the risk message positively or, indeed, negatively? These matters should

figure large in the calculations of a government faced with managing the perception and communication of risk on a society-wide scale.

Opportunity and security. New technology is often associated with new risks and opportunities. Understanding what the new opportunities might be for the rogue insider or for the criminal outsider with access to IS, makes the work of confounding their efforts much easier. The opportunity model discussed in Section 3, the second study, could be used in staff education and awareness programmes by emphasizing their role in supporting guardianship. One of the problems faced by organizations is gaining employee cooperation in maintaining effective security. Lack of cooperation is often the result of staff failing to appreciate the vital role they play, especially when they perceive security as solely the task of those people directly responsible for security (Wood 1995). However, one of the facets of the opportunity model is its ability to emphasize the centrality of staff behaviour in providing effective guardianship over an IS. This suggests that education programmes could, for example, be used to highlight the need for compliance with local security policies. Such a relationship could be described in terms of simple offender, target and guardianship relationships. Examples could be imported from criminology (for example, guardianship over property and personal belongings) to help highlight the 'informal' role people can play in crime prevention programmes.

The Crime Specific Opportunity Structure model is a conceptual tool that can enable organizations to identify elements that may afford a collective control environment and to highlight the relationships between the components of the collective. This perspective provides a potential alternative to technocratic approaches to IS security. Further research is required to assess the feasibility of this model, but introducing a criminological perspective opens the way for transfusions into security thinking from insights from social science research. The opportunity structure model permits a systematic and coherent framework to be introduced, linking all those organizational functions whose work is central or tangential to security – risk, IS security, audit, compliance, human relations and so on, fostering an integrative or joined-up approach to the management of risks. Working in isolated 'silos' has been a problem for modern corporate functional divisions of labour, when information flows 'up' functions, rather than 'across' them, thereby hindering coordinated attacks on the problems.

Internal control systems. In the context of large-scale relocation of company operations to developing countries such as India and Thailand, the issues of internal control and security are key ones. In section 4, the third study, within an audit approach to internal control a semiotic framework was applied to reveal important issues about control in decentralized organizations relying on a pervasive technical infrastructure. As the tentacles of cyber organization reach ever further into the recesses of the global environment, the issue of control looms larger than ever. Empirical research is needed on the tradeoff between the facility with which the technical side of cyber systems can be developed and the more difficult establishment of operational norms among different participant cultures and sub-cultures. Formal rules developed in the corporate headquarters may not be implemented or inscribed into the informal systems of the operations in other countries in the manner expected. A focus on developing management tools and techniques drawing insight from a variety of theoretical frameworks must be a priority if control systems are to be strengthened in the future.

Interoperability. As the growth of networks supports greater interaction among businesses and government bodies, the question looms as to the security of the systems and procedures of potential collaborators. This is explored in Section 5, case study four. Not only must there be the technical capacity to interoperate, there needs to be interoperation at the level of the institution, its policies and practices. Collaboration usually requires giving access to users whose identities have been authenticated elsewhere and whose access rights must be reconciled with those of the 'home' organization. The technical problems have not been simple to resolve, but the institutional trust issues are proving even more intractable. The study of the take-up of PKI reveals the labyrinth of issues that arise within the confines of two global corporations. Both these organizations participate in many initiatives aiming to develop industry interoperability, yet both have had considerable problems in achieving that goal internally. The obstacles were never simply technical, but always involved the cultural and political dimensions of the organizational information systems. There has been an evolution in security issues from concern about technical devices, such as cryptography and firewalls, to management issues. This evolution is evidenced in the success of

the code of information security management BS7799, and ISO17799, the international standard that it spawned. The next phase of security approaches is likely to focus on the interoperation of management policy. This will require new theoretical frameworks that can address the issues.

7 CONCLUSION – SOCIAL SCIENCE CONTRIBUTIONS

The failure of the *c:cure* accreditation scheme (Backhouse et al. 2003) and, arguably, the muted success of *tScheme*,⁴ the UK's supervisory scheme for trusted third parties, underline the problems of approaching policy issues in security from technical and regulatory angles without considering sufficiently the social and political agendas. Although there was strong support for the use of PKI and digital certification to underpin identity management in the West (NIST 2000), nothing like the progress expected has been achieved. The social sciences have a contribution to make in framing the problem and offering solutions. Security issues are never simply technical questions that can be underpinned by law and regulation. In the area of web services and identity and authentication, a range of (technical) protocols is being established that are predicated on an entity accepting the trusted credentials from another.⁵ What is missing are the business and trust protocols to provide the institutional level of mutual confidence. In the near future, it is likely that ratings service providers, such as Standard and Poor's and Moody's, will offer credit rating-style operational risk ratings to short-cut the process of deciding at what level to trust certain counter-parties. This may be followed by cyber risk ratings for insurance purposes along the lines of the operational risk ratings that are emerging with respect to Basel II Capital Accord.⁶ Making a market in security risk might prove to be the quickest route to enabling interoperability of electronic identities. Longer term security planning is likely to require that a variety of insights from the social science disciplines is brought to bear on the problems raised by identity and authentication issues.

7.1 Cross-disciplinary Focus

Opportunities need to be created for cross-disciplinary collaboration on the topic of security and risk. Traditional IS security research groups will need to work with entities such as the Jill Dando Institute and University College London, with their focus on crime reduction. The Institute focuses on the application of criminology to reduce crime and includes eminent scholars such as Ron Clarke, who has been a pioneer in the development of the 'criminal opportunity' approach discussed in Section 3. A current proposal is to develop the criminal opportunity model for application to information systems security risks, building from the work of Willison (2002), in an effort to design crime out of systems and procedures. A suitably tested and researched model might be the basis for a risk management framework that could be taught to managers as 'best practice' in the area. As e-government and e-business take off, there will be greater opportunities for criminals to insinuate themselves into the crevices of such systems. They will seek to exploit design loopholes and to profit from tactics such as identity theft, the supply of false credentials and the like. If systems and procedures are conceived *ab initio* as 'low criminal opportunity zones', then significant reductions could be achieved in cyber crime. Many electronic systems are now being devised to take advantage of cyber working so there will be scope to deploy collaborations of this kind.

7.2 Qualitative Research in Security

Qualitative research of the kind reviewed here has an important role to play in information security. Yet the preconception that real security is about technology continues to linger. The realization that secure systems rely as much on social as technical factors is only slowly being established in the research and practitioner community. Qualitative, interpretive research can be rigorous and it addresses the recognition, meaning and interpretative aspects of risk. These are the baseline competences for contingency planning, security awareness and prompt preventive action. In a complex social system, a technically conceived security system will never replace the richness of a human and informal system, augmented by a formal control framework and supported by pervasive ICT. As the concern of business, government and the practitioner community focuses on the development of an appropriate culture of security, social science research will need to be undertaken to provide practical frameworks based on the results of theoretical and empirical work.

7.3 Future Research Topics

A number of possibly fruitful research topics emerge from this review and with consistent methodologies would yield useful results for those concerned about cyber risks and cyber security.

The semantics of security – to aid the sharing of data on security and the interoperability of policy, some fundamental concepts of the subject need to be properly mapped out and a logic of security behaviour determined. Currently terms such as risk, attack, event, threat, and vulnerability mean different things to different entities. An interpretive or hermeneutic study aimed at analyzing the meaning of these terms and the development of an ontology of the discourses employed in security debates would facilitate communication and policy development.

Signalling security and trustworthiness - a detailed analysis of how security and trustworthiness is signalled successfully in an open global environment still remains to be undertaken. Application of semiotics and signalling theory from economics would be a most valuable support to research in this area.

The well chosen epigram - 'Security ... depends on balancing cost and risk through the appropriate use of technology and policy'⁷ which captures the essence of the pragmatic approach subscribed to in this paper, suggests two further areas for research.

One focuses on the notion of balancing cost and risk and, increasingly, reward – where, for example, a successful Basel II rating frees up risk capital for use in the business. Here, we could imagine a methodology for investigating the effects of different (portfolio) management strategies applied in the search to avoid underprotecting assets or overspending on countermeasures.

The other research area centres on the interplay between technology, policy and, arguably, informal culture and tries to develop, with an interpretivist study, greater understanding of the term 'appropriate' and so inform management who must decide about such tradeoffs.

7.4 Emphasizing the Social Context of Security

Rejecting the view that security problems in cyberspace are caused by fallible humans and resolved by infallible technology, the aim in this paper has been to draw attention to the social context in which security risks arise and may be resolved. While new technology always alters the social context in which it is introduced and triggers new risks, the accumulated evidence of qualitative research suggests that gradually efforts are made to accommodate the benefits and mitigate the disadvantages of the technology by altering behaviour appropriately. Security managers must grapple with the best combinations of technology, policy and behaviour. Good progress has been made on the first two – the greatest need now is to turn attention to the last member of this trinity.

NOTES

- 1 See Morgan (2003).
- 2 Peter Baring, *Financial Times* 28 Feb. 1995.
- 3 The PKIX Working Group was established in the Autumn of 1995 with the intention of developing Internet standards needed to support an X.509-based PKI, <http://www.ietf.org/html.charters/pkix-charter.html>, accessed 17 Apr. 04.
- 4 At the present time only five Approved Services have been accredited, the first one dating from 11 Feb. 2002, <https://www.tscheme.org/directory/index.html>, accessed 17 Apr. 04.
- 5 e.g. www.projectliberty.org or www.pingid.com, both accessed 17 Apr. 04.
- 6 See <http://www.aba.com/Industry+Issues/RiskBasedCapital2.htm>, accessed 17 Apr. 04.
- 7 See Economist (2002).

REFERENCES

- Audit Commission (1994), *Opportunity Makes a Thief: An Analysis of Computer Abuse*, London: Audit Commission Publications.
- Audit Commission (1997), *Ghost in the Machine: An Analysis of IT Fraud and Abuse*, London: Audit Commission Publications.
- Audit Commission (2001), *Your Business@Risk: An Update on IT Abuse 2001*, London: Audit Commission Publications.

- Backhouse, J. (1997), 'Information@Risk', *Information Strategy Online* 4(Jan.): 33-35.
- Backhouse, J., Hsu, W.Y. and McDonnell, A. (2003), 'Toward Public Key Infrastructure Interoperability' *Communications of the ACM* 46(6): 98-100.
- Bartlett, C. and Goshal, S. (1989), *Managing Across Borders: The Transnational Solution*, Boston MA: Harvard Business School Press.
- Bener, A. (2000), 'Risk Perception, Trust and Credibility: A Case in Internet Banking. Information Systems', London School of Economics and Political Science.
- BloomBecker, B. (1984) 'Introduction to Computer Crime', in J. Finch and E. Dougall (eds) *Computer Security: A Global Challenge*, Amsterdam: North-Holland/Elsevier.
- Board of Banking Supervision (1995), 'Report of the Board for Banking Supervision Inquiry into the Circumstances of the Collapse of Barings', London: HMSO.
- Bologna, J. (1993), *Handbook on Corporate Fraud*, Boston MA: Butterworth-Heinemann.
- Brantingham, P.J. and Brantingham, P.L. (1991), *Environmental Criminology*, Prospect Heights IL: Waveland Press.
- Chauvidul, N. (2003), 'Formality and Informality in Internal Control Systems: A Comparative Study of Control in Different Social and Cultural Environments in a Global Bank', Department of Information Systems, London School of Economics and Political Science.
- Chokhani, S. and Ford, W. (1998), 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework', RFC 2527, <http://www.faqs.org/rfcs/rfc2527.html>
- Clarke, R. (1995), 'Situational Crime Prevention' in M. Tonry and D. Farrington (eds) *Building a Safer Society. Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research*, Chicago IL: University of Chicago Press, pp. 91-150.
- Clarke, R. (1997), *Situational Crime Prevention: Successful Case Studies*, Albany NY: Harrow and Heston.
- Clarke, R. and Cornish, D. (1985), 'Modelling Offender's Decisions: A Framework for Policy and Research' in M. Tonry and N. Morris (eds) *Crime and Justice: An Annual Review of Research*, Chicago IL: University of Chicago Press, pp. 147-85.
- Clarke, R. and Cornish, D. (2000), 'Rational Choice', in R. Paternoster and R. Bachman (eds) *Explaining Crime and Criminals: Essays in Contemporary Criminological Theory*, Los Angeles CA: Roxbury Publishing Company, pp. 23-42.
- Clegg, S.R. (1989), *Frameworks of Power*, London and Newbury Park CA: Sage.
- Comer, M. (1998), *Corporate Fraud*, Vermont VA: Gower.
- Cornish, D. and Clarke, R. (1986), 'Situational Prevention, Displacement of Crime and Rational Choice Theory' in K. Heal and G. Laycock (eds) *Situational Crime Prevention: From Theory into Practice*, London: HMSO, pp. 1-16.
- Courtney, R. (1977), 'Security Risk Assessment in Electronic Data Processing', *AFIPS Conference Proceedings of the National Computer Conference*, Arlington VA: AFIPS Press, pp. 97-104.
- Dorey, P. (1994), 'Security Management and Policy', in W. Caelli, D. Longley and M. Shain (eds) *Information Security Handbook*, London: Macmillan, pp. 27-41.
- Douglas, M. (1985), *Risk Acceptability According to the Social Sciences* New York: Russell Sage Foundation.
- Economist (2002), A Survey of Digital Security, *The Economist*, 26 Oct.
- Ellison C. (1997) 'What Do You Need to Know About the Person With Whom You Are Doing Business?' Written testimony of Carl M. Ellison to the US House of Representatives Science and Technology Subcommittee, Hearing of 28 October 1997: Signatures in a Digital Age, <http://world.std.com/~cme/html/congress1.html> (accessed 13 Nov. 2003)
- Ernst & Young (2002), 'Global Information Security Survey Presentation Services', Ernst & Young,

London.

- Felson, M. (1992), 'Routine Activities and Crime Prevention: Armchair Concepts and Practical Action', *Studies on Crime and Crime Prevention* 1(1): 31-34.
- Fesseden-Raden, J., Fitchen, J. and Heath, J.S. (1987), 'Providing Risk Information in Communities: Factors Influencing What is Heard and Accepted', *Science, Technology and Human Values* 12(3/4): 94-101.
- Fitzgerald, J. (1978), 'EDP Risk Analysis for Contingency Planning', *EDP Audit Control and Security Newsletter* 6(Aug.): 1-8.
- Forester, T. and Morrison, P. (1994), *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, Cambridge MA: MIT Press.
- Hinde, S. (2001), 'The Weakest Link', *Computers & Security* 20(4): 295-301.
- Hindelang, M., Gottfredson, M. and Garafalo, J. (1978), *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*, Cambridge MA: Ballinger.
- Hirschi, T. (1969), *Causes of Delinquency*, Berkeley and Los Angeles CA: University of California Press.
- Hitchings, J. (1995), 'Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology,' *Computers & Security* 14(5): 377-83.
- Hofstede, G. (1991), *Cultures and Organisation - Software of the Mind. Intercultural Cooperation and its Importance for Survival*, Columbus OH: McGraw-Hill.
- Krimsky, S. and Plough, O. (1988), *Environmental Hazards: Communicating Risks as a Social Process*, Dover MA: Auburn House.
- Luzwick, P. (2001), 'Security? Who's Got Time For Security? I'm Trying to Get my Job Done', *Computer Fraud & Security* 1:16-17.
- McDonald, G. (2000), 'Cross-Cultural Methodological Issues in Ethical Research', *Journal of Business Ethics* 27(1/2): 89-104.
- Morgan, O. (2003), 'Swipe Strike Cost BA £50M', *Observer/Guardian*, <http://observer.guardian.co.uk/business/story/0,6903,1006430,00.html>, accessed 17 Apr. 04.
- National Institute for Science and Technology (2000), 'Federal Agency Use of Public Key Technology for Digital Signatures and Authentication', National Institute of Standards, NIST Special Publication 800-25, October, <http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf>, accessed 17 Apr. 04.
- National Research Council (1989), *Improving Risk Communication, US Committee on Risk Perception and Communication*, Washington DC: National Academies Press.
- Nosworthy, J. (2000), 'Implementing Information Security in the 21st Century - Do You Have the Balancing Factors?' *Computers & Security* 19(4): 337-47.
- Olnes, J. (1994), 'Development of Security Policies', *Computers & Security* 14(8): 628-36.
- Osborne, K. (1998), 'Auditing the IT Security Function', *Computers & Security* 17(1): 34-41.
- Parker, D. (1997), 'The Strategic Values of Information Security in Business', *Computers & Security* 16(7): 572-82.
- Riem, A. (2001), 'Cybercrimes of the 21st Century', *Computer Fraud & Security* 4: 12-15.
- Schneier, B. (1998), 'Security Pitfalls in Cryptographic Design', *Information Management & Computer Security* 6(3): 133-37.
- Skibell, R. (2002), 'The Myth of the Computer Hacker', *Information, Communication & Society* 5(3): 336-56.
- Spurling, P. (1995), 'Promoting Security Awareness and Commitment', *Information Management & Computer Security* 3(2): 20-26.

- Stevenson, G. (2000), 'Computer Fraud: Detection and Prevention', *Computer Fraud & Security* 11: 13-15.
- Thomson, M. and von Solms, R. (1998), 'Information Security Awareness: Educating Your Users Effectively', *Information Management & Computer Security* 6(4): 167-73.
- Thorne, L. and Saunders, S.B. (2002), 'The Socio-Cultural Embeddedness of Individual's Ethical Reasoning in Organisations', *Journal of Business Ethics* 35(1): 1-14.
- von Solms, B. (2001), 'Corporate Governance and Information Security', *Computers & Security* 20(3): 215-18.
- Wamala, F. (2002), 'Comparing Public Key Infrastructure Institutionalisation in Two Global Organisations', The Fiducia Project, Department of Information Systems, London School of Economics and Political Science.
- Warman, A. (1993), *Computer Security Within Organisations*, London: Macmillan.
- Wasilewski, N. (2002), 'An Empirical Study of the Desirability and Challenges of Implementing Transnational Marketing Strategies', *Advances in Competitive Research* 10(1): 123-49.
- Willison, R. (2002), 'Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank', Department of Information Systems, London School of Economics and Political Science.
- Willison, R. and Backhouse, J. (2003), 'Understanding Criminal Opportunity in the IS Context', paper presented at the Information Systems Research Seminar in Scandinavia IRIS 26 Conference, 9-12 August, Haikko, Finland.
- Wood, C. (1995), 'Writing InfoSec Policies', *Computers & Security* 14(8): 667-74.
- Wright, M.A. (2001), 'Keeping Top Management Focussed', *Computer Fraud & Security* 5: 12-14.
- Yapp, P. (2001), 'Passwords: Use and Abuse', *Computer Fraud & Security* 9: 14-16.