AUTHOR(S): MITCHELL, R.C., MARCELLA, R. and BAXTER, G.

TITLE: Corporate information security management.

YEAR: 1999

Publisher citation: MITCHELL, R.C., MARCELLA, R. and BAXTER, G. 1999. Corporate information security management. New library world [online], 100(5), pages 213-227. Available from: http://dx.doi.org/10.1108/03074809910285888

Corporate Information Security Management

Ruth C. Mitchell, Rita Marcella and Graeme Baxter
School of Information and Media
The Robert Gordon University, Aberdeen

Abstract: *To ensure business continuity the security of corporate information is extremely important. Previous studies have shown that corporate information is vulnerable to security attacks. Companies are losing money through security breaches. This paper describes an MSc project that aimed to investigate the issues surrounding corporate information security management. Postal questionnaires and telephone interviews were used. Findings indicate that companies are not proactively tackling information security management and thus are not prepared for security incidents when they occur. Reasons for this lack of action include: awareness of information security threats is restricted; management and awareness of information security is concentrated around the IT department; electronic information is viewed as an intangible business asset; potential security risks of Internet access have not been fully assessed; and surveyed companies have not yet encountered security problems, therefore are unprepared to invest in security measures. The recommendations include that companies: carry out a formal risk analysis; move information security management from being an IT-centric function; and alter perceptions towards electronic information so that information is viewed as a valuable corporate asset.*

Keywords Information security, Electronic information resources, Companies

Introduction and background

The potential effects of a breach of information security are all too clearly illustrated by a recent 'hacker' attack through the Internet on a Massachusetts airport, which disabled the control tower, communications, and emergency systems for 6 hours (Festa, 1998b). Corporate information security breaches, although less dramatic, can also have devastating effects. The loss of proprietary product information, client data, or strategic business plans can result in the loss of customers and credibility, even causing operational breakdown, and ultimately affecting profitability.

Companies may be viewed as communications systems (Backhouse and Dhillon, 1995), where the success of a business is dependent on its ability to organise its information and communications, both internally and externally. Electronic information systems are fundamental to the operation of most companies, whether they are multinational corporations or small retailers (Dhillon, 1997). Given its significance, securing corporate information from unwanted disruption should have become of critical importance.

Securing electronic information was simpler in the days of mainframes: with hundreds of dumb terminals connected to a huge central computer, all that was necessary was to protect access routes to the one central information repository. Then came the Personal Computer (PC) and Local Area Networks (LANs) where data moves two ways from the LAN server to hundreds of PC's. The complexity of this information system compounded security problems; however, as the majority of users were physically internal to the organisation the security threats remained containable. Today, the threats are multiplied by connection to the Internet: just as every individual connected to the Internet is a potential customer or supplier, they are also a potential security threat (Pfleeger, 1997). Computer based fraud, sabotage and vandalism of information, and theft of proprietary information are just a few of these threats.

Studies by the National Computing Centre (NCC) revealed that almost half of the British companies surveyed had suffered at least one serious information security breach, costing on average £7,146, rising to more than £20,000 for companies with over 500 employees (NCC, 1998). The Department of Trade and Industry (DTI) predicted that "threats to information security are expected to become more widespread, more ambitious and increasingly sophisticated" (British Standards Institution, 1995, p1).

While management processes, policies and technologies exist to protect corporate information, there is still evidence to suggest that companies are either unaware of the scale of the threats, or are not taking steps to protect information. With this in mind, it was decided to investigate attitudes to information security amongst commercial organisations in the UK. This investigation was conducted, by the first named author above, as part of the requirements of the Master of Science Degree in Information Analysis at the Robert Gordon University's School of Information and Media in Aberdeen. The main aims of this study were to:

- establish the current issues surrounding information security management;
- investigate current attitudes to information security amongst key decision-makers in commercial organisations; and

- identify current corporate practices and procedures with regard to information security management.

Methodology

Literature Review

Information security management is concerned with ensuring business continuity and minimising business damage by preventing and minimising the impact of security incidents that threaten an organisation's information assets (British Standards Institution, 1995). The three basic components of information security are to maintain:

1) confidentiality of sensitive information, protecting it from unauthorised disclosure or intelligible interception;
2) integrity, safeguarding the accuracy and completeness of information; and
3) availability, ensuring that information and vital services are available to authorised users when required. (Pfleeger, 1997).

Information security management systems are the mechanisms which protect information stores and thus enable the implementation of information security (British Standards Institution, 1995).

Davies and Price (1989) argued that every major advance in technology changes the concept of securing information. Following a study into computer crime in the UK, the Audit Commission (1998) concluded that the Internet could become the security challenge of the millennium. A study carried out by the Computer Security Institute found that 68% of respondents had suffered a security breach within the previous year, a rise of 16% from 1997 (Wilson, 1998). This growing trend is illustrated by other studies. The 1997 Global Information Security Survey (Davis, 1997), for example, found that:

- 47% of US respondents reported losses of up to $100,000 due to viruses.
- 52% of Canadian respondents had suffered financial losses due to a security breach during the year, 13% of these losing at least $100,000.

The 1998 Global Information Security Survey found that companies already engaging in electronic commerce over the Internet experience three times the number of incidents resulting in information loss or theft of trade secrets (Dalton, 1998).

A threat to information systems can be defined as "circumstances that have the potential to cause loss or harm" (Pfleeger, 1997, p3). This loss could consist of the absence of data or a resource within an information system, financial loss, or loss of company credibility. Threats can either be singular or form part of a combination of multiple threats. Hendry (1995) and Warman (1993) classified information security threats as follows:

- *Passive threats* are unpredictable natural or physical disasters and accidental human errors occurring completely at random, such as fires or floods. 'Clueless' or apathetic

users also constitute a primary threat to information security (Schuman, 1996). The Millennium Bug is, perhaps, the most visible example of a passive threat.

- *Active threats* are deliberate and malicious attacks on information systems. These can potentially be predicted and avoided. They may be carried out by insiders or outsiders (Pfleeger, 1997), and they may be the result of direct or indirect action.

The most commonly known and frequent type of active threat is the 'hacker'. It is estimated that a different computer on the Internet is hacked into every 20 seconds (Taylor, 1997). Hackers also carry out 'denial of service' attacks (Radcliff, 1997), bombarding central network computers with a large number of e-mail messages that cause the computer to overload and shut down. The University of Minnesota was recently attacked (Festa, 1998a), suffering information losses as computers shut down and setting up a chain reaction throughout the State.

Indirect information system penetration involves the use of a "tool within the computer [which] is used to attack or further open a known weak point in the overall system" (Warman, 1993, p12). There are four major types of indirect threats to information systems:

(1) a worm is a program that, once established on a computer, spreads copies of itself through a network;
(2) a Trojan horse is a program claiming to carry out a non-malicious activity which, once activated, takes on a malevolent aspect (Pfleeger, 1997);
(3) logic bombs are a class of malicious computer program, activated when a specified condition occurs, such as a date (Pfleeger, 1997); and
(4) a virus 'infects' other programs by embedding a copy of itself without the users' knowledge.

Some 13,000 virus strains have been identified, of which approximately 230 are circulating and able to do harm. The rest exist as 'virus samples' in secure research labs around the world (Davis, 1997; Pallato, 1998).

If a threat to a corporate information system is realised, then the nature of the damage to information can be of the following types: (Pfleeger, 1997; Warman, 1993).

- *interruption*, where an information asset becomes lost, unavailable or unusable;
- *interception*, where an unauthorised party gains access to an information asset;
- *modification*, where an unauthorised person not only accesses but also tampers with an information asset; or
- *fabrication*, where an unauthorised party introduces counterfeit objects to an information system

Companies have legal obligations as well as commercial reasons for securing electronic information. In the UK, one of the principles set out in the Data Protection Act (1998) is that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." Despite the potential consequences of not protecting information, KPMG found, in their 1998 Information Security Survey, that 1 in 5 UK organisations surveyed were

not registered under the Data Protection Act, even though the simplest information system, such as that for payroll, processes personal data. The US and UK governments have also considered the potential threat of 'information warfare': that is the "deliberate and systematic attack on critical information activities to exploit information, deny services to the authorised user, modify or corrupt data" (Hobby, 1996; Goodin, 1997).

The 1995 British Standards Institution *Code of Practice for Information Security Management Systems*, (BS 7799) described a set of security controls recommended as good corporate practice. Ten key management controls were highlighted in the standard, which constitute the minimum requirements for any organisation. These were:

1. Information security policy document, indicating the goals of information security.
2. Allocation of information security responsibilities. One method suggested by Wood (1996) involves naming information 'owners', 'custodians', and 'users'.
3. Information security education and training programmes for all staff.
4. Reporting of security incidents, formally ensuring that all employees are aware of procedures.
5. Virus controls implemented to detect and prevent viruses.
6. Business continuity planning, identifying risks to business operations and developing plans to ensure critical business processes continue to run in the event of disaster.
7. Control of proprietary software copying to ensure that only software developed by or licensed to the company is used.
8. Safeguarding of organisational records to protect them from loss, destruction and falsification.
9. Data protection: registering with the Data Protection Registrar and ensuring that information is used only for genuine business purposes.
10. Compliance with security policy to be regularly monitored throughout an organisation, and all elements of information security management analysed periodically.

In order for companies to be able to demonstrate their commitment to security, the DTI, the United Kingdom Accreditation Service (UKAS), and the British Standards Institution (BSI) developed an accreditation scheme for companies compliant with British Standard BS7799. However, shortly after its introduction, KPMG conducted a national survey which revealed that only 2% of the 1500 companies surveyed had implemented the standard, and over half of the respondents did not know of its existence (Lambeth, 1996a). This study also found that 60% of the respondents failed to realise that they were connected to the Internet, and that 65% of firms did not know how their employees were using the Internet (Kerridge, 1996).

In 1998, KPMG carried out a similar survey and found that 8% of respondents had adopted the Standard, with a further 12% intending to implement. However, KPMG concluded that organisations had not improved their information security management over the intervening two years (KPMG, 1998).

There are a growing number of guides available, providing instructions on how to secure corporate information assets when connected to the Internet (for example, Atkin (1996), Vacca (1996) and Varleys (1996)). Professional security organisations have also published

practical recommendations (for example, the Computer Security Institute, 1997). The Internet is also a rich source of information: organisations such as the National Institute of Standards and Technology (NIST) in the US and the National Computing Centre in the UK provide information on security products, advice on policy, and a vast number of links to other security related sites. The Computer Emergency Response Team (CERT) is one of the largest sites with services to help companies across the globe (Sanderson and Forcht, 1996).

Postal questionnaire

A postal questionnaire was selected as the primary research instrument in order to gain as broad a view as possible of the issues surrounding information security, amongst a spectrum of companies from a wide geographical area. Questionnaires also enabled a degree of anonymity and confidentiality that was desirable, as it was felt that information security may be a sensitive subject to some corporations. The questionnaire sought to establish how companies are managing the security of their electronic information, and to determine what factors influence attitudes and behaviour. The questionnaire was piloted amongst 20 companies across a range of industry sectors. Seven pilot questionnaires were returned and the questionnaire was modified as appropriate.

A sampling frame of approximately 1,500 companies from nine industry sectors was drawn up from the *FAME* database and Yahoo's *UK Company directory list.* Questionnaires were then sent to a sample of 200 companies using systematic sampling. Distribution of these forms took place in March 1998. It should be re-emphasised here that the research was conducted as part of a student dissertation, therefore the survey sample size was necessarily limited, due to constraints of time and resources. Forty completed questionnaires were returned: a response rate of 20%. This was a below average response rate for a postal questionnaire, perhaps because of the sensitivity of the subject. However, responses were received from all industry sectors surveyed, and from a variety of different sized companies; and while the low response rate means that the participants' responses and contributions could certainly not be regarded as being truly representative of UK industry, it is believed that the results are sufficiently illustrative of current trends in, and attitudes to, corporate information security management. Completed questionnaires were coded and analysed using the Microsoft *Excel* software package; this initial analysis highlighted the areas that required further investigation.

Interviews by telephone

To achieve a greater understanding of information security issues within companies, it was decided to carry out a number of semi-structured telephone interviews. The interview schedule evolved from the analysis of the questionnaire responses. The number of questions was limited so that the interview would not last more than 30 minutes, and to reduce bias questions were clearly phrased and open. The questions were intended to act as prompts throughout the interviews so that conversation would flow naturally and in the direction the interviewee wished to take.

Eleven IT managers indicated on their returned questionnaire that they would be willing to take further part in this research, and interviews were arranged with four individuals. During each interview notes were taken on a printed schedule, and these notes were then transcribed for analysis into recurring themes. The responses fell into two categories: actions and influencing factors. Therefore, data displays were used to map the relationships between the actions and the influencing factors (Hussey & Hussey, 1997). The interviews generated much useful information that illuminated the trends highlighted by the questionnaires. Again, however, as so few organisations were interviewed, the results cannot be generalised to all companies.

Results and Conclusions

Questionnaire survey results

As already indicated, 40 questionnaires were completed and returned. Respondents were primarily drawn from the manufacturing (22.5%), general trade (17.5%) and finance (17.5%) sectors (see Figure 1).

Take in Figure 1

Meanwhile, the respondent company size, by number of employees, was as follows:

- 50 employees 43%
- 51 - 150 employees 23%
- 151 - 499 employees 18%
- 500 employees 13%

Electronic corporate information

The majority of companies responding to the survey had embraced IT and electronic information (see Figure 2). Only two companies had 25% or less of their corporate information stored electronically. Most of the respondents (68%) stored over half of their business information in electronic format, with 43% keeping more than three quarters of their information electronically. The general trade sector had the highest proportion of respondents (five out of seven companies) with more than 75% of their business information held electronically. Only a small proportion of respondents (five companies) did not know how much information their company stored electronically, although interestingly two of these respondents were responsible for managing their corporate information stores.

Take in Figure 2

IT infrastructure

The respondents were asked to give the number of PCs or work stations installed at their site. When this number was compared with the number of employees at that site, it was seen that 76% of companies potentially had a PC for each employee. Hence the majority of employees in each of the respondent companies could have personal and immediate access to corporate electronic information stores. The respondent companies operate in a highly networked environment: 95% of respondents were using LANs to interconnect their PCs or workstations; 19 companies (48%) were using private wide area networks (WANs), and six of these were coupling this with Intranet technology.

Internet connectivity and use

Some 93% of respondents were connected to, and were using, the Internet. The number of connections ranged from 1 PC to corporate wide access through a LAN. For the vast majority of respondents, the number of connections did not reflect the number of employees. One exception was the largest company to return the questionnaire (3,000 employees in the financial services sector) which gave all employees access. The primary purpose of Internet access was e-mail, followed by information research (see Figure 3). The 'other' uses of the Internet were for interactive customer service (finance sector company) and electronic commerce (general trade company).

Take in Figure 3

Responsibility for management of electronic information

In half of the companies surveyed, responsibility for the management of information stores lay with a member of the IT department (see Figure 4). In 20% of the companies the responsibility belonged to operational functions, such as product management or engineering. In a quarter of the companies the responsibility was with senior management, i.e. Director level or higher. Only two companies replied that no-one was responsible for information management; interestingly, both were from the construction industry.

Take in Figure 4

Responsibility for information security

Only two of the respondent companies had an information security manager responsible for the security of their corporate information; both of these companies were in the financial services sector. As Figure 5 illustrates, 57.5% of the respondents had placed the responsibility for the security of electronic information with the IT department. The financial

service sector differed in that only two respondents placed responsibility for security with IT. Seventeen companies had the same person in charge of information security and information management. Only one company (again, a small company from the construction industry) had no-one formally taking responsibility for information security. Interestingly, none of the respondents indicated that an Information Manager was responsible for managing or securing corporate information, perhaps suggesting that companies see electronic information in terms of the technology and not within an information manager's domain.

Take in Figure 5

Classification of corporate information

Respondent companies used a variety of ways to classify the security of their corporate information. The most common methods were:

- configuration management (25%), identifying and controlling the changes to data, reporting the changes throughout each item's life cycle, and controlling the configuration of the information system; and
- security ratings (25%), classifying each item of information according to a management defined security level, so that information receives an appropriate level of protection. For example, classification might range from open access (available to all) to completely closed access such as highly confidential (controlled access).

The least used classification method was document/data numbering (15%), that is identifying each piece of information with a unique code. Six companies reported that no procedures were in place to classify the sensitivity of their stored electronic information; these included the two largest companies (over 2,500 employees). Nine of the respondents did not know which procedures their company used.

Methods used to assess security risks to corporate information appeared to be informal and cautiously applied. On average, each respondent company used one procedure to identify and assess threats to their corporate information stores. The most common procedure (60% of respondents) used to evaluate information security threats was on an 'as required' basis, where, for example, a security breach or a change in IT infrastructure might cause a company to assess the security risks posed to their corporate information. These companies might be deemed flexible, or simply reactive and ill-prepared. Fewer than a quarter of these companies combined ad hoc risk evaluation with any proactive risk analysis methods. (Risk analysis is a formal process by which security exposures are determined and their potential harm assessed in terms of cost (FT Financial Publishing, 1997); by carrying out risk analysis regularly, companies can form a complete picture of the risk they are exposed to and be more aware of the dangers). This trend of appraising threats only when required was consistent across all industry sectors, except in the financial services sector where six out of the seven respondents took a more formal approach and identified and assessed information security threats using either systematic risk analysis or as part of their auditing process. Two respondent

companies, including one of the largest companies to respond, used no method at all to assess threats to stored electronic information,.

Formal information security policies

Of the 40 companies, only 17 had any kind of written corporate policy statement regarding the security of their stored electronic information. This suggests that fewer than half of the respondents had incorporated information security into everyday working practices and that information security was not a high priority. As Figure 6 illustrates, the majority of the companies with security policies were in the finance or manufacturing sectors. The finance sector had the highest proportion of responding companies (five out of seven) to have a policy.

Take in Figure 6

Statistical tests using the chi-square test also showed that, at the 99% confidence level, the size of the company was related to the existence of an information security policy. Figure 7 illustrates that as the size of the company increased the more likely the company was to have a formal policy.

Take in Figure 7

Eleven of those companies with an information security policy indicated that they review and modify their policy ‘as required’, and five companies indicated that they modify it annually. In the computer industry, general trade, and manufacturing sectors, the majority of companies with a policy alter it ‘as required’. However, there was more variety amongst the respondents from the finance sector (one twice a year, two annually, two as required). Interestingly, the two companies from the finance sector to reply ‘as required’ both had more than 1,000 employees, indicating that perhaps larger companies need to be more flexible in their approach to information security policy.

When asked for details about what their policy covered:

- 12 companies indicated that their policies take into account third party access to corporate information systems. Two companies did not allow any third party access at all.
- 11 companies explained that the policy includes business continuity plans for use in the event of a security breach.

Employees’ awareness of information security policies

Just under half (eight) of the companies with information security policies felt that the employees in their company were 'quite aware' of the policy, with four reporting that their employees were 'very aware'. On the other hand, two companies believed that their employees were 'not at all aware'. The financial services had the highest proportion of 'very aware' employees, whilst the general trade sector showed the poorest level of employee awareness. The existence of policy does not significantly impact on employee behaviour, as only eight companies indicated that working practices were affected by policy.

Training and education

The BS7799 Code of Practice (1995) recommended that employees should be trained in corporate security procedures and policies, including their responsibilities, the use of software packages, and how to report security incidents. However, the proportion of respondent companies that had ongoing programmes of security education and training for employees was very low. Only 13 out of the 40 respondents (32.5%) indicated that they give information system security training to their employees. The manufacturing industry had the highest proportion of respondents carrying out formal security training.

Statistically, there was no connection between training provision and whether or not a company had an information security policy document. In other words, the existence of a formal policy document did not mean that the company was translating policy into action. However, the importance, and indeed effectiveness, of combining policy with user training was illustrated by those companies that had a formal security policy. As Figure 8 shows, the level of employee awareness of corporate information security policy increased for those companies which gave training. More companies also claimed that working practices were affected by policy, if their employees had received training.

Take in Figure 8

Perceived threats to information security

Computer failure (80%) and fire (80%), closely followed by computer viruses (75%), were considered to be the most serious security threats. On average, each respondent regarded five out of the nine possible threats given in the questionnaire as significant (see Figure 9). However, two companies (including one of the largest companies to reply) did not believe that any of these options were a threat; unfortunately they did not give reasons for this belief. A third of the respondents felt that their corporate information security was at risk from disgruntled employees. In comparison, 50% believed mistakes by authorised employees threatened security. Only 40% of the respondents felt that that the Internet was a serious threat to their corporate information stores. This is perhaps surprising when taking into consideration the current level of media coverage of the security risks that the Internet presents.

Take in Figure 9

Practical counter measures employed

Although a high proportion of respondent companies did not have a formal information security policy, they all used safeguards to protect their electronic information stores. The most common security measure involved controlling access to information, either physically or utilising technology. However, reliance on technical security measures was higher than on physical measures.

Physical measures

On average, three different physical security measures were used by each of the respondent companies (see Figure 10). However, this number ranged from as many as seven to none: two companies reported that they provided no physical protection for their information systems. The most frequently used precaution was remote back up and storage of electronic information (85%), followed by computer access control (70%). The least popular method of physically securing information systems was found to be the marking of equipment and movable data storage. The 'other' security measures cited included strong boxes for servers, door locks and alarms on buildings, and electronic access for staff: all of which might be classed as 'computer access control'. One respondent also mentioned disaster recovery by a third party. While 80% of the respondents considered fire to be a serious threat to their corporate information, only 45% were specifically protecting information systems from fire. Of the 32 companies which perceived fire as a threat, 27 (84%) used remote back up and storage as a method of physically protecting their electronic information.

Take in Figure 10

Technological measures

On average, each respondent company concurrently used four different technological measures to secure their information system (see Figure 11). Two companies used only one technical safeguard - virus controls. Indeed, protection against computer viruses was the most commonly applied (88%) security measure. Virus scanners can be used to automatically detect and eliminate viruses on a computer before the virus can spread any further. Not surprisingly, the questionnaire results showed that, statistically, implementation of specific virus protection was positively related to perceptions of virus threats.

Some 83% of respondents used some form of application access control within their corporate information system, while 80% of respondents used some form of network access control, such as passwords.

Take in Figure 11

Software can be used to monitor user activity on an information system or corporate network: for example, failed attempts to log on or to access files can be monitored. Forty per cent of the responding companies used such system monitoring tools. Financial services showed the highest proportion of usage, although interestingly none of the computer industry respondents used these methods.

A firewall provides a barrier between an internal, corporate network and a less trustworthy or external network. Effectively, the firewall enables communication from the inside out, but not from the outside in. Some 33% of respondents used this type of security safeguard. Again, the finance sector significantly showed five of seven companies using firewalls. A router is the simplest form of firewall (Pfleeger, 1997), through which all electronic messages into and out of a corporate network or a section of a network are passed. The router filters each 'piece' of a communication, therefore information flow can be monitored and controlled by configuring the router. Only 35% of respondent companies used routers.

Companies can ensure that each user ID for their information system can only be active, or in use, from one point at any time. This is known as single sign on, and 30% of the respondents used this method to secure corporate systems.

Encryption is a process by which information is 'scrambled' using a mathematical algorithm so that its content is no longer obvious. The information can then only be read by a person in possession of a key which can 'unscramble' it. Only a quarter of the respondents used encryption techniques to secure their corporate information, making encryption the least used method. Companies from the financial sector showed the highest proportion of use of encryption (four of seven companies).

Only one company (from financial services) used any other technical safeguards. These were software licence monitoring, software audit alert tools, and sophisticated authentication devices such as smart cards.

Although the average number of security precautions taken and the existence of an information security policy were statistically independent, it can be seen, in Table 1, that the respondent companies with a formal policy document did implement slightly more physical and technological precautions than those companies without a policy. The financial services sector, on average, used more software security precautions than any other sector.

Take in Table I

Impact of information security breach

Over 50% of respondents believed that a breach of information security would have 'some impact' on their company's business. This might imply that they were confident in the security measures that they were taking, or that the extent of the damage from an information security breach was unpredictable and variable depending on its nature. Risk analysis techniques might help them to estimate the potential costs of a breach. Three companies indicated that an information breach would have 'negligible impact' on their business, while 12 companies believed a breach would have 'extensive impact' on their business. The companies from the computer industry showed the highest proportion believing that a breach would have extensive impact. It might be hypothesised that this sector were more aware of the possibilities.

Frequency of actual security breaches

Thirty-five respondents (87.5%) stated that their information system had not been breached by an unauthorised person external to the company. No respondents were aware of their company having been hacked into. Five respondents were open enough to admit that they did not know. Breaches are only known if the hacker caused visible damage, and it may be that greater numbers than stated so are unaware of such incidents.

Telephone interview results

Brief portraits of the four companies interviewed are presented in Table II.

Take in Table II

Current practices and procedures

For all companies interviewed, access to their electronic information was restricted to a 'need to know basis'. Each employee's log-on ID and passwords identify them within the corporate information system and grant them access to the information that is relevant to their job. Information can only be modified by authorised users.

In three of the companies interviewed (A, C and D), ownership of electronic information was allocated to the area that primarily administers that information. For example, in Company A the employees are arranged into work groups, and each work group has access to, and uses, information that is relevant to them. Security of particular information is the responsibility of the work group(s) that can access it. All three of these companies argued that, despite this type of formal control, ownership of information was still a 'grey' area, particularly when two or more different user groups used the same information and responsibility had to be taken for inaccurate or out of date information. Company B differed from the other three in that they had no procedures for assigning ownership of information, the reason for this being that they were a small company and believed that they could identify who was responsible for each piece of information, if necessary.

All four companies had a full-time team of employees dedicated to the maintenance and development of their information systems. However, only Company B (the company without a security policy) had a formal emergency business continuity plan for use if the company suffered any kind of disaster. With regard to corporate information, the success of the plan relied on back-up tapes of the system being removed from the business site each night. In the event of a physical disaster, the back-up tapes would be used to reinstall the system on a single computer and selected staff would be able to use it. However, the plan did not include what they would do if they were hacked into from the Internet.

None of the companies had a specific information security training programme. Employees were given IT training only on the part of the system that they used. In Company C, employees attended user group meetings, to teach them about IT matters and to communicate corporate IT policy. However, security of information systems was not part of the training programme discussed in these groups. The reasons were given as follows:

- IT staff did not have the time nor resources to spend on training that was not viewed as necessary by senior management.
- training employees to use the corporate system correctly was seen as enough to prevent mistakes being made.

Attitudes towards information security

Companies A, C and D all indicated that security of their corporate information was a high priority for their company, but that more could be done. The IT manager in Company B had no hesitation in replying that information security was not a priority in their company.

When asked 'what does your company think is the biggest threat' to their information, the majority of interviewees, personally, thought that external logical threats, such as hacking and remote access, were the greatest threats. However, they reported that these views were not held throughout the rest of the company as, generally, the security of electronic information was viewed in terms of physical damage to the computers.

The interviewees in the three companies with an information security policy (A, C and D) believed that, over the previous five years, their personal awareness of information security issues had increased, as a result of new staff bringing knowledge into the company and perceptions amongst IT staff having matured. The IT manager from Company B did not think that the company as a whole were any more security conscious now, than they were five years ago.

In the opinion of the interviewees, employees throughout the four companies were largely unaware of information security issues, and security policies were regarded as just 'another piece of admin'. The IT managers also believed that most of the staff did not have the technical ability, nor interest, to try to electronically breach information security.

The factors that influenced these companies' attitudes towards information security were felt to be:

- *Ownership of the company.* Foreign ownership affected three out of the four companies interviewed. In particular, two companies had US parent companies and this appeared to heavily influence management of, and attitudes towards, information security. In both cases, the implementation of their corporate information security policy was initiated and driven by the parent companies. It was indicated that Company A's parent company has an internal audit team which regularly assesses the UK company's security procedures on a rolling cycle basis, examining different parts of the system each time. This team visits the UK annually to fully audit the system and update corporate policy accordingly.

- *No perceived cost benefit in investing in information security.* None of the interviewed companies had suffered a serious information security breach (i.e. one that has cost them money), either physically or electronically. Therefore, it was perceived to be of little benefit to invest in further resources to protect information.

- *Lack of resources* within IT departments or the company as a whole, to police employees and enforce policy, meant that awareness of security issues was not communicated throughout the company.

- *'Hasn't happened in the 25 years that we have been in business' attitude.* Companies had not suffered any major information security breaches and so assumed that it would not happen in the future. Therefore, there was little sense of urgency in creating corporate policy and implementing further security controls.

Investment in information security was generally regarded as likely to increase very gradually. Only a security breach or an upgrade of information system would spark off heavy investment and changes in corporate policy. Company D indicated that if company wide access to the Internet were to be introduced, investment would be made in a firewall. Although the four companies were not currently engaged in electronic commerce with any of their suppliers or customers, Company D were considering it for the future. If they did begin trading on-line, then the interviewee believed that security of their information system would be carefully considered as their IT system was upgraded.

Competitive environment and management culture

Interviewees from Companies A, B and C, from the general trade sector, felt that the competitive environment that they operated in did not affect their corporate attitudes to information security. Company D, in the manufacturing industry, believed that fear of information falling into competitors' hands was an influencing factor. Indeed, a minor security incident, involving employees moving to a competitor company, had been one of the reasons why they had developed their corporate information security policy.

Information security policies had been introduced relatively recently. While the reasons for creating a policy varied, all companies wanted to provide their employees with a formal reference point for security issues. The department initiating information security policy was not always IT: in one company the policy was managed and controlled by the Human Resources function, while the IT department managed and maintained the technical security aspects. When it came to enforcing the policy, two interviewees (Companies A and C) were vague about how their company might go about it. Company D stated that if someone broke the information security rules then normal company disciplinary procedures would apply.

None of the companies interviewed had a specific forum or committee that dealt only with information security issues. Companies C and D, who had recently introduced policies, would deal with security matters in regular managerial meetings. (In both companies, as part of implementation, the policy was distributed to each employee, who then had to return a signed form indicating that they had read and understood the policy). In the other two companies (A and B), memos and e-mails were the most common methods used to advise employees on security issues. Company D had also placed their information security policy document on their corporate Intranet site along with other company procedures. They were currently in the process of making it part of employee contracts that they must be aware of all company policies, and any changes to them. Therefore, theoretically, employees had to read the policies on the Intranet.

Corporate information

All four companies use their information system to store business critical information. They indicated that information flows within these systems provide the backbone to their business operations. For example, Company A use their system to connect all of their UK outlets and to manage and control stock. Every aspect of the business is managed through the system: purchasing, distribution, sales, stock control and finances. All of the companies were involved in either the manufacturing or supply and servicing of goods, and so their information systems were similar.

Two of the interviewees (C and D) believed that, as a company, their corporate information was viewed as a valuable asset. However, there was an underlying implication from both of these interviewees that, although this was the ‘official line’, the reality was that the company probably did not value information as highly as other assets, such as the computers that the information was stored on. The IT Manager at Company B, which did not have a formal information security policy, believed that the Company did not view their information as a valuable asset, replying that “the fact that it is always there means that they take it for granted”.

The Internet

All of the companies interviewed were connected to the Internet, although only Company B allowed corporate wide access to it. The others restricted access. Connection to the Internet had meant that these organisations had taken limited consideration of the risks it exposed

them to. Company A indicated that being connected to the Internet had meant that they were more aware of the 'holes in their system'. All of the IT Managers appeared aware of the risks that the Internet posed, although they felt that their company was secure from these threats. Only Company B believed that being connected to the Internet had made no difference to their attitude to security, because the general feeling was 'it will not happen to us'.

Conclusions

The findings of the present research project suggest that the majority of companies were reactive in managing information security, despite the fact that electronic information was important to the operation of their business. In the event of a security breach, companies were likely, therefore, to be unprepared, and for business damage to be greater than it might have been.

The financial services sector demonstrated a marked difference in awareness of information security, implementation of policy and protective measures. The factors that differentiated this sector from the others appeared to be that traditionally preserving customer confidence and the integrity of business information were fundamental to these companies' business. Therefore, corporate credibility and valuable information assets were identified as key driving factors in the implementation of sound information security management procedures.

The questionnaires and interviews uncovered several reasons for this apparent lack of interest in information security in the other industry sectors. Firstly, electronic information was viewed as an intangible business asset and therefore hard to value. Companies were not carrying out formal risk analyses, so the potential cost of a security breach was often unknown.

Awareness of information security threats was found to be restricted to understandable threats where the potential damage was easily conceived. Perceptions of the Internet as a threat were low, despite the fact that all companies surveyed were connected to the Internet.

In the surveyed companies, management of information security was concentrated around the IT function. IT managers were largely responsible for managing and securing electronic information, and a variety of technological security precautions were being implemented. It would appear that information security was viewed as a technology problem to be dealt with by technology people. However, the softer issues of corporate policy, employee training, and communication were also important, for knowledge, awareness and commitment to information security issues to spread throughout the company. This resulted in gaps in the corporate information security chain of defences.

The Internet had not yet become an essential part of the surveyed companies' business operations. This may explain why these companies had not yet considered all the risks that the Internet poses and taken appropriate steps to protect themselves. In the meantime, however, they were still connected to the Internet and exposed to the threats.

The primary reason that companies were not taking more action to protect corporate information was that they had not yet experienced any major security breaches, especially from the Internet. Hence there were no perceived cost benefits in implementing further security measures or corporate policies.

Overall findings showed a very limited approach to electronic information security management, where companies were only able to deal with issues reactively, and implement security measures when it was too late to save money, company credibility and customers.

The results of this research would suggest that companies should:

a) carry out a formal risk analysis assessing all possible security exposures and quantifying the potential costs to the company. This will enable informed policy formulation that meets business needs.
b) move information security management from being an IT-centric function and put security on everyone's agenda, thus encouraging 'buy in' from all management and operational functions.
c) encourage the view that information is a valuable corporate asset and treat it as such. This may be demonstrated through the achievement of (a) and (b) above, which will result in the raising of the profile of information security.

By carrying out these three recommendations, companies will prevent or be prepared in the event of future information security attacks. They will also be flexible enough to implement new technologies and change working patterns as information security threats become ever more complex.

References

Atkins, D. *et al* (1996), *Internet Security: Professional Reference*, New Riders Publishing, Indianapolis.

Audit Commission (1998), *Ghost in the Machine: an Analysis of IT Fraud and Abuse*, Audit Commission, London.

Backhouse, J. and Dhillon, G. (1995), "Managing computer crime: a research outlook", *Computers and Security*, Vol. 14**,** pp. 645-651.

British Standards Institution (1995), *BS7799: Part 1, Information Security Management: Code of Practice for Information Security Management Systems*, BSI, London.

British Standards Institution (1998), *BS7799-2, Information Security Management: Specification for Information Security Management Systems*, BSI, London.

Computer Security Institute (1997), *The CSI Manager's Guide to Information Protection*, CSI Publications, San Francisco.

Dalton, G. (1998), "Acceptable risks", *InformationWeek*, 31 August, pp. 36-48.

Davies, D.W. and Price, W.L. (1989), *Security for Computer Networks*, 2nd ed., John Wiley & Sons, Chichester.

Davis, B. (1997), "Security survey: is it safe?", *InformationWeek*, 8 September, p. 42.

Dhillon, G. (1997), *Managing Information System Security*, Macmillan Press, Basingstoke.

Festa, P. (1998a), "Smurf attack hits Minnesota", *CNET News.com*, 17 March.
Available at http://www.news.com/News/Item/0,4,20178,00.html [Accessed April 1999]

Festa, P. (1998b), "Airport hack raises flags", *CNET News.com*, 19 March.
Available at http://www.news.com/News/Item/0,4,20278,00html [Accessed April 1999]

FT Financial Publishing (1997), *Financial Crime and Security on the Internet*, FT Financial Publishing, London

Goodin, D. (1997), "Taking aim at cyberterrorism", *CNET News.com*, 22 October.
Available at http://www.news.com/News/Item/0,4,15516,00.html [Accessed April 1999]

Great Britain, House of Commons (1998), *Data Protection Act 1998*, HMSO, London.
Available at http://www.hmso.gov.uk/acts/acts1998/19980029.htm [Accessed April 1999]

Hendry, M. (1995), *Practical Computer Network Security*, Artech House, Boston

Hobby, J. (1996), "Cyber leeches", *Computer Weekly*, 5 December, p. 46-47.

Hussey, J. and Hussey, R. (1997), *Business Research: a Practical Guide for Undergraduate and Postgraduate Students*, Macmillan Press, Basingstoke

Kerridge, S. (1996), "Firms fall short of national standard on data security", *PC User*, Vol. 279, 20 March, p. 14.

KPMG (1998), *Information Security Survey 1998*, KPMG, London

Lambeth, J. (1996a), "Why security is failing to meet the standard", *Computer Weekly*, 14 March, p. 18.

Lambeth, J. (1996b), "Time to get serious about data security", *Computer Weekly*, 21 March, p. 4.

National Computing Centre (1998), *Business Information Security Survey*, NCC, Manchester

Pallato, J. (1998), "Anti-virus scanners: defending the network domain", *Internet Computing*, April. Available at http://www.zdnet.com/products/content/zdim/0304/287180.html [Accessed April 1999]

Pfleeger, C.P. (1997), *Security in Computing*, 2nd ed., Prentice Hall International, New Jersey.

Radcliff, D. (1997), "Hackers, terrorists, and spies", *Software Magazine*, October. Available at http://www.sentrytech.com/97issues/Oct99/sm107cv.htm [Accessed April 1999]

Sanderson, E. and Forcht, K.A. (1996), "Information security in business environments", *Information Management and Computer Security*, Vol. 4, No. 1, p. 32-7.

Schuman, E. (1996), "Main threat to Net security? Clueless user", *Communications Week*, 16 September, pp. 24-6.

Taylor, P. (1997), "How ethical hackers pinpoint security weaknesses", *Financial Times Technology Section*, 3 September, p. 1.

Vacca, J. (1996), *Internet Security Secrets*, IDG Books World wide Inc., Foster City

Varleys, J. (Ed). (1996), *Safeguarding Electronic Information*, McFarland & Company Inc., Jefferson, N. Carolina.

Warman, A.R. (1993), *Computer Security within Organizations*, Macmillan Press, Basingstoke

Wilson, T. (1998), "Profits embolden hackers", *InternetWeek*, 23 March. Available at http://internetwk.com/news/news0323-4.htm [Accessed April 1999]

Wood, C.C. (1996), “Information owners, custodians, and users”, *Information Management and Computer Security*, Vol. 4, No. 4, pp. 34-5.

The authors

Ruth C. Mitchell is a Consultant in the e-business group of Computacenter, London, UK.

Rita Marcella is a Reader and the Depute Head of School at the School of Information and Media, The Robert Gordon University, Aberdeen, UK.

Graeme Baxter is a Research Assistant within the School of Information and Media, The Robert Gordon University, Aberdeen, UK.

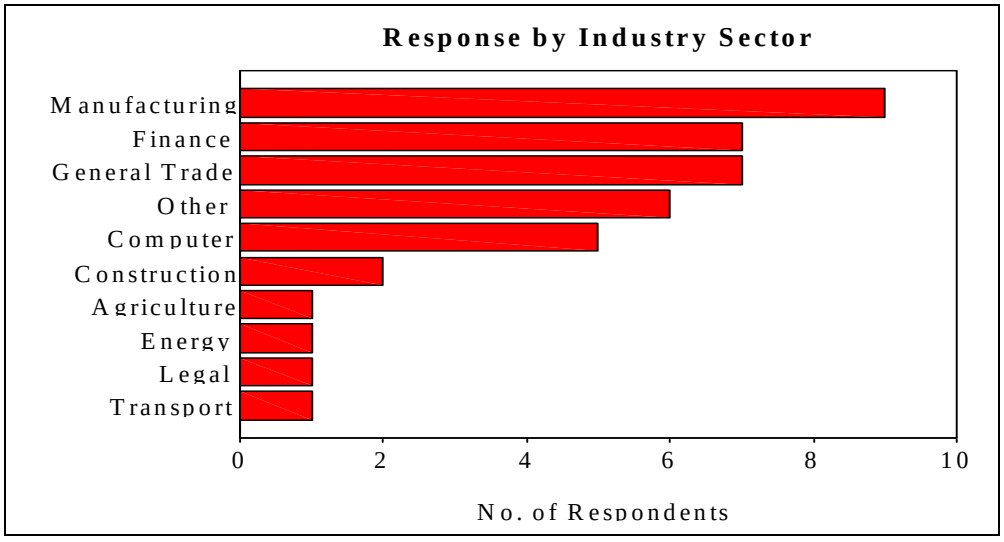

Figure 1

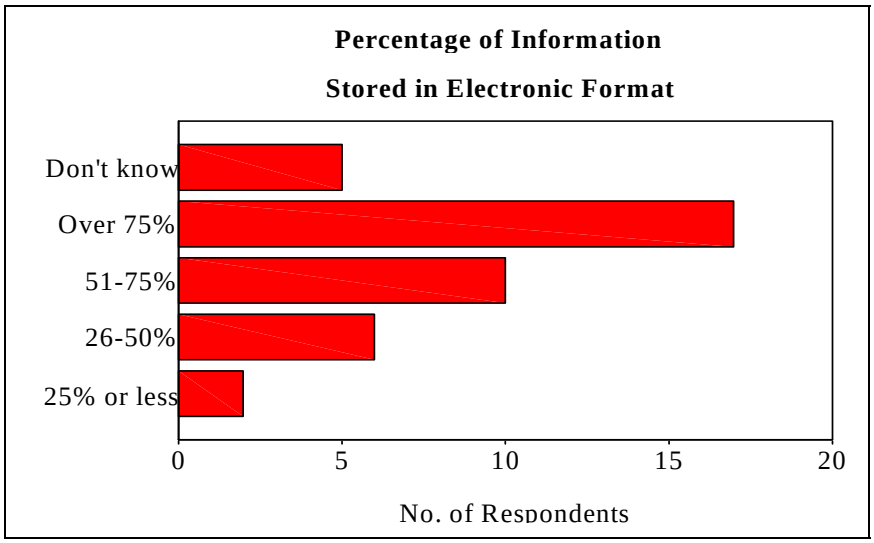

Figure 2

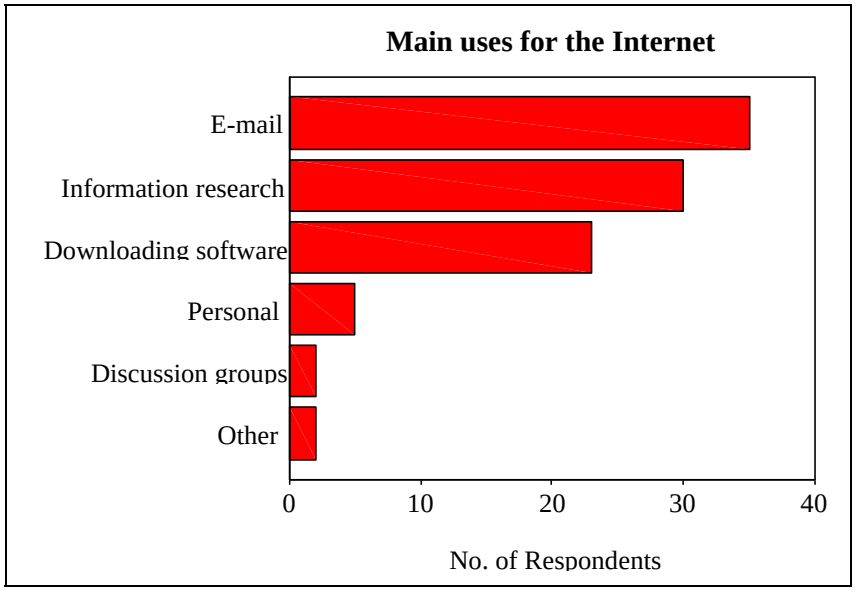

Figure 3

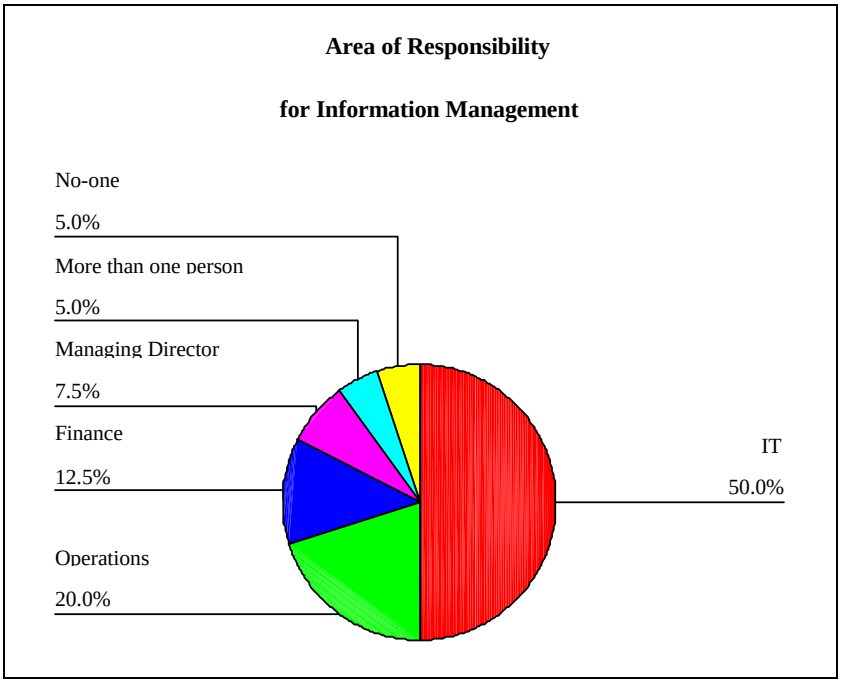

Figure 4

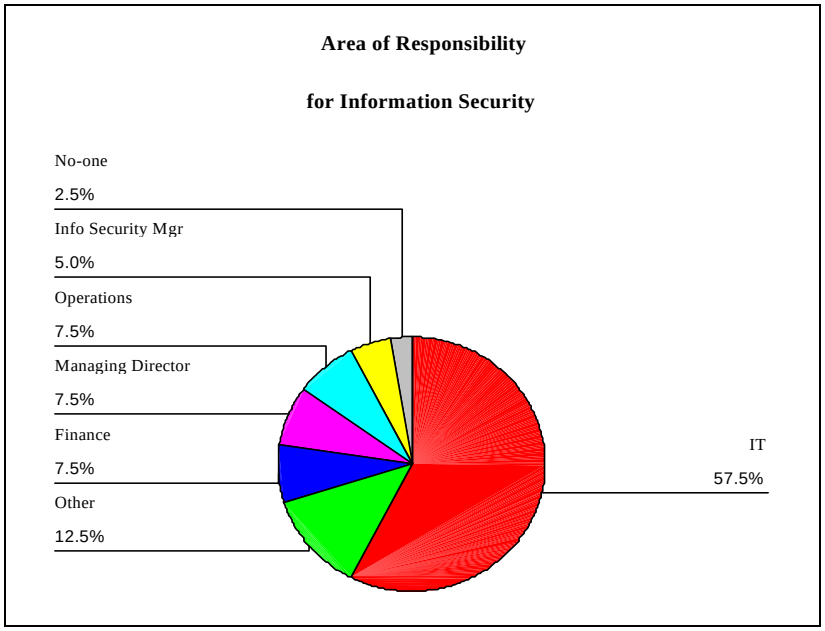

Figure 5

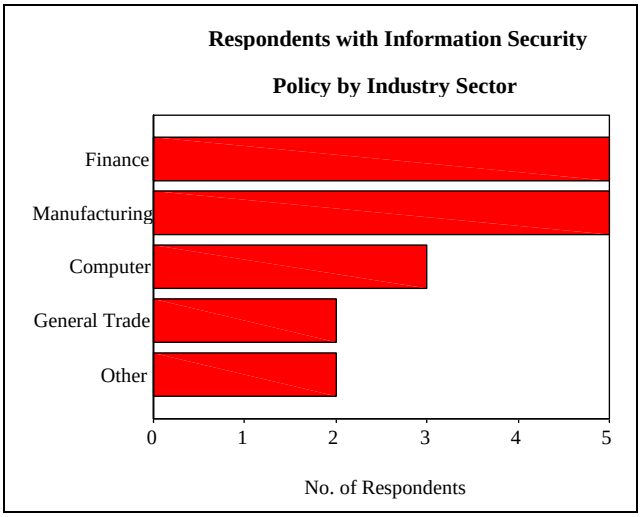

Figure 6

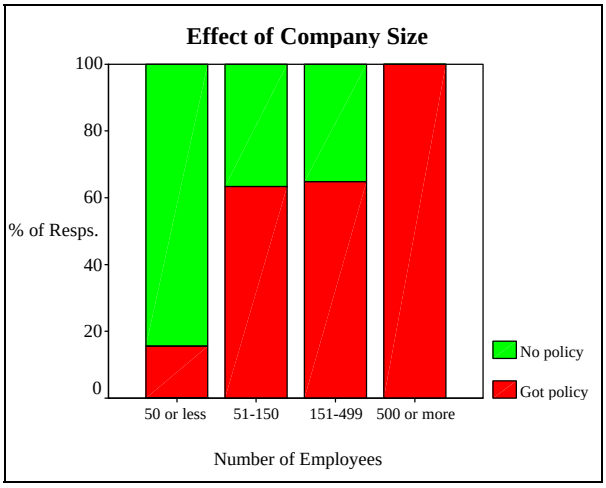

Figure 7

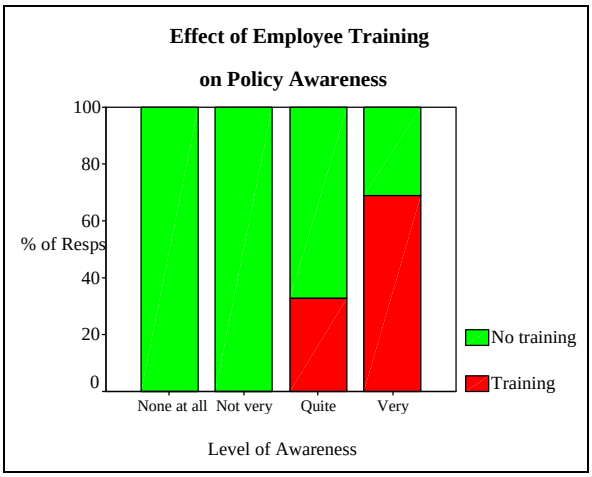

Figure 8

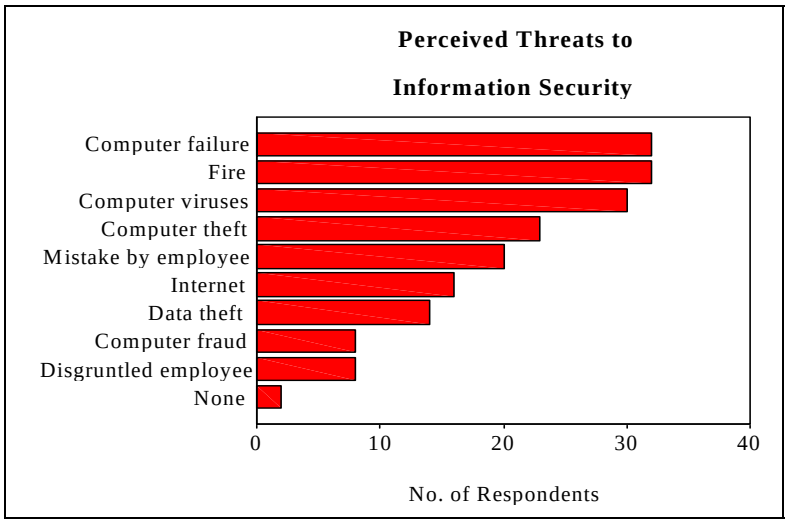

Figure 9

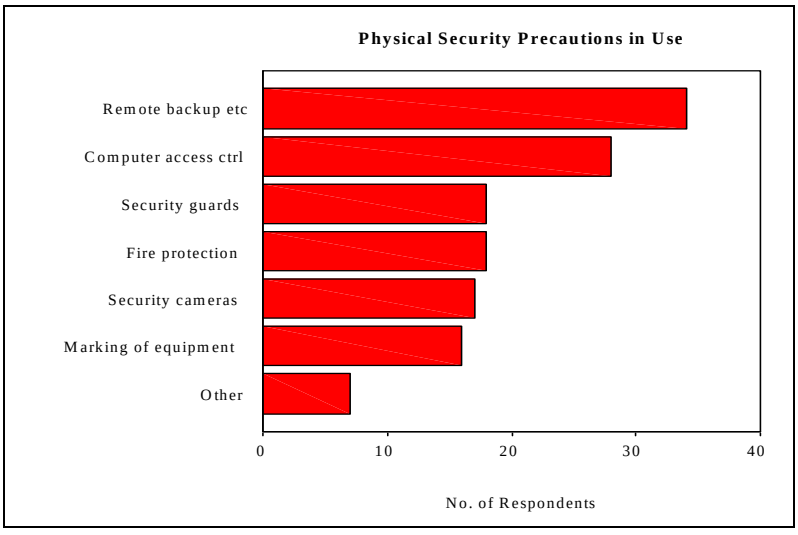

Figure 10

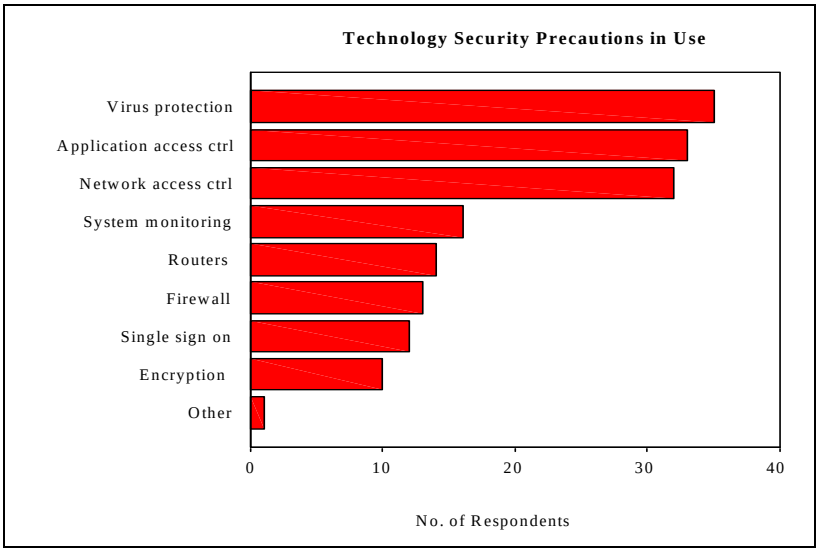
Technology Security Precautions in Use
Virus protection
Application access ctrl
Network access ctrl
System monitoring
Routers
Firewall
Single sign on
Encryption
Other
0
10
20
30
40
No. of Respondents

Figure 11

	With policy	No policy
Average number of physical precautions	4	3
Average number of technical precautions	5	3
Total	**9**	**6**

Table I

Company	Description	No. of Employees	Information Security Policy?	Policy Status
A	A clothing retailer established in the UK five years ago. The company is owned by a large US firm and operates over 30 shops throughout the UK.	140	Yes	Implemented one month before interview following six months in draft.
B	A subsidiary of a Japanese company that has been operating in the UK for 25 years. The company sells and distributes bearings within the UK only. The 50 employees primarily comprise sales staff.	50	No	n/a
C	Involved in the sales and servicing of photocopiers and fax machines. The company was formed with the merger of three separate companies and is owned by a US company.	250	Yes	Introduced within the last year as part of revising the entire corporate policy documents.
D	From the manufacturing	100	Yes	Introduced

	industry sector, this independent company was established in the mid 1970s and its primary function is the design and manufacture of modular units for the offshore oil and nuclear energy industries. The company has several offices in Europe and operates on a global scale.			within the last year as part of an IT policy document.

Table II