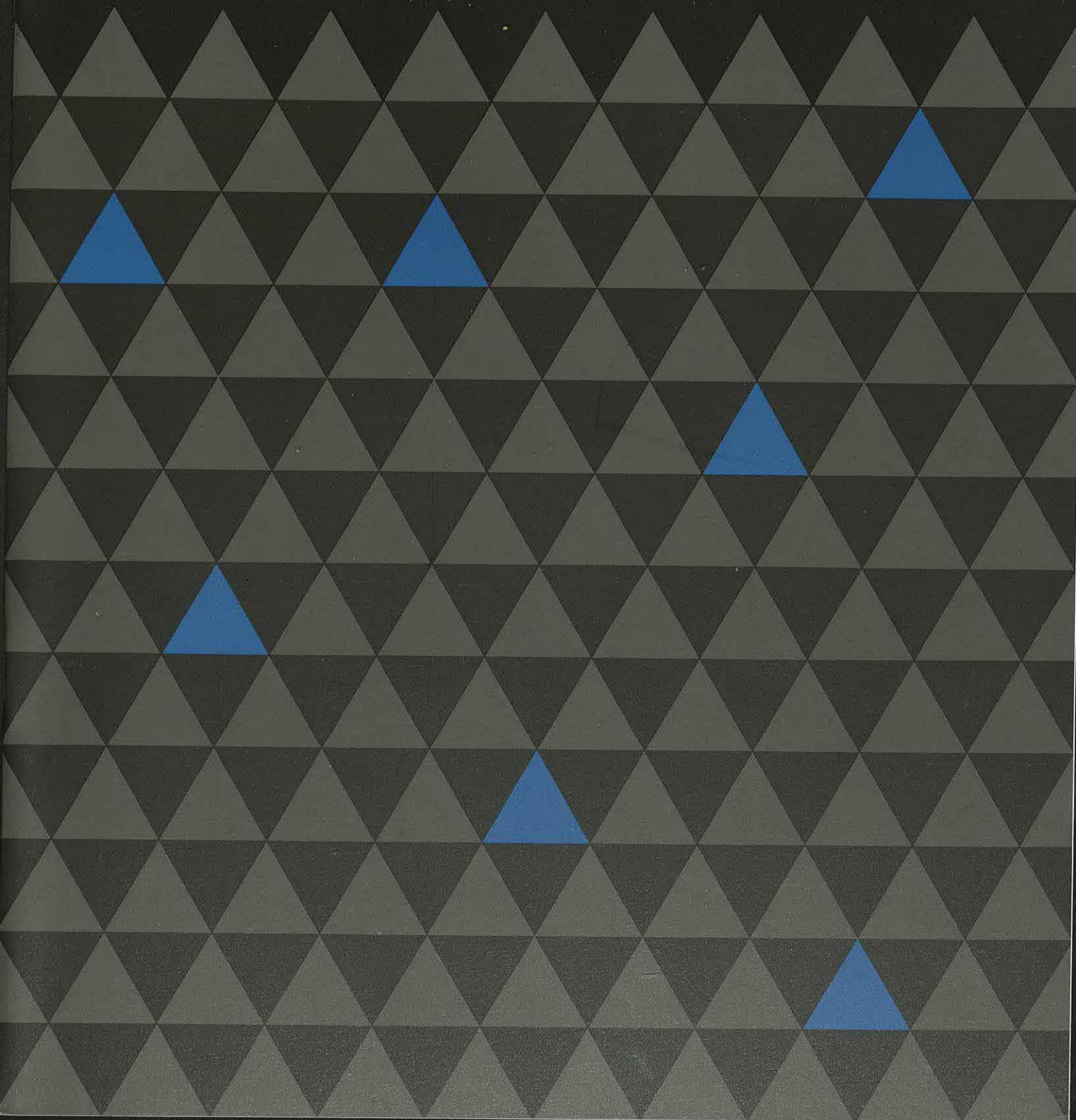
Legal Protection for Computer Systems

BUTLER COX FOUNDATION

A Paper by Emma Nicholson, MP
September 1989



BUTLER COX FOUNDATION

Legal Protection for Computer Systems

A Paper by Emma Nicholson, MP
September 1989

Emma Nicholson is the Conservative Member of Parliament for Devon West and Torridge. She is one of only a handful of MPs with a background in computing, having joined ICL in 1963 where she trained and worked as a programmer and software designer. Subsequently, she worked as a computer consultant for John Tyzack, and as a computer and general consultant for McLintock, Mann & Whinney Murray. Her interest in computing has continued in Parliament, where she is now a council member of PITCOM (Parliamentary Information Technology Committee). She sat on the Committee that scrutinised the Copyright, Designs and Patents Act 1988, and was instrumental in introducing amendments and new clauses that have major implications for the computer industry. In 1989, she launched a campaign and introduced a Bill to outlaw hacking and to control computer misuse and electronic eavesdropping.

In July, Miss Nicholson addressed UK members of the Butler Cox Foundation at the House of Commons. This paper is an edited transcript of her presentation. It has been supplemented by the results of a subsequent survey of UK Foundation members. This survey shows that Foundation members fully support Miss Nicholson's view that there is an urgent need for legislation to control the misuse of computer systems.

Published by Butler Cox plc
Butler Cox House
12 Bloomsbury Square
London WC1A 2LL
England

Photoset and printed in Great Britain by Flexiprint Ltd., Lancing, Sussex.

BUTLER COX FOUNDATION

Legal Protection for Computer Systems

A Paper by Emma Nicholson, MP
September 1989

Contents

Legal Protection for Computer Systems

Most people are aware of the damage that can be done to organisations by unauthorised interference with their computer systems. Computers provide criminals, malicious employees, and even undisciplined students, with novel opportunities for fraud, sabotage, prying into private information, and misuse of systems. These threats have been discussed in the past and are well documented in the publications listed in the bibliography at the end of this paper.

It is less well known, however, that government departments are rapidly computerising, not just their own internal procedures, but the consumer services they provide to the electorate. The computer systems that are being set up to administer the collection of the community charge, and the creation of new systems to store and process medical records are two significant examples. Because of the sensitivity of the information that will be held in these types of systems, the Government is becoming aware of the importance of systems security.

Hacking affects individual citizens

For me, the real significance of the community charge is that, for the first time, personal information now held separately in a number of sources is being drawn together and held locally on a single computer record. Because, for example, of the 'tapering' system under which one in four of the population will get a rebate of some description, a considerable amount of personal information will be held by District Authorities, which could be accessed for unofficial purposes.

In West Lothian and another Scottish District, hackers claim to have deleted the records of live people, and replaced them with records of people who have died, which means that the community charge will not be collected from the live people whose records have been deleted. The community-charge systems in these councils keep failing and no-one is sure if the failures are caused by the hackers or by poor system design. The police have been called in to investigate.

There are also concerns about the misuse of computerised medical records. Such records are becoming increasingly common as more and more GPs install personal computers. Once the District Health Authority hospital records have been computerised, the GPs' records may be linked in. After all the Health Authorities have been computerised, which is supposed to happen before 1991, the records may be available regionally and then nationally online.

These developments will improve the treatment available to patients because doctors will be able to share, and build on, the knowledge gained from different cases. However, there are also substantial potential disadvantages. For example, there have been cases in France where the computerised records of blood donors have been improperly accessed, and AIDS victims, whose records are, of course, marked because they are not suitable for donating blood, are being blackmailed. There have also been two cases (again in France) where a computerised intensive-care system was interfered with. Two patients have died as a result of this unauthorised access to a computer system.

I am very concerned about computerisation in hospitals because people are going to be very vulnerable if the information stored about them is misused or is used in an unauthorised way. I already know of two cases in which information obtained from medical records has been misused:

— The first concerns a cancer victim who had not shared that knowledge with her family

and friends. Somebody has found out, through access to her electronically stored record, and is blackmailing her.

— The second concerns a lady who is separated from her husband. Her new-born baby has some problems that she did not want her husband to know about. He found out the details of the birth and is harassing her because of this.

These examples illustrate that there is increasing public concern about the misuse of government computer systems. The results of the Butler Cox survey, and other surveys such as my own, demonstrate that the business community is equally concerned about the misuse of computer systems.

Business is seriously concerned

The responses to the Butler Cox survey showed that both private- and public-sector organisations are seriously concerned about the threat to systems security. (Details about the survey are contained in the appendix and are summarised in Figure 1.). The Butler Cox survey was not available at the time of my talk. However, my own survey, published earlier in July, gave similar findings, albeit more dramatic, on the hacking front.

The current law is inadequate

The present position under British law is that an unlawful act, such as theft, fraud, or criminal damage, is still unlawful if it is done through a computer system. It is probable that displaying obscene material on a bulletin board is not illegal. I hope the new Broadcasting Bill may take this in (the Home Secretary indicated this in response to my Parliamentary Questions on the topic). However, intrusion into a computer system, in the absence of any criminal act, is neither a crime nor a civil wrong, and British law provides no sanctions against the perpetrator of such an intrusion. In addition, data corruption or insertion is not a criminal act and the planting of viruses, time bombs, worms, Trojan horses, et al is therefore not illegal, nor is the alteration of records stored electronically. British law therefore covers cases where the computer is the channel for an offence but not those where it is, in effect, the victim.

The new Copyright Act does make it illegal to copy software but, since it is only a civil law, a fine of £2,000 is the maximum penalty.

Another problem arising from the lack of a British anti-hacking law is illustrated by the fact that I had to quote French examples of computer misuse. France has had a law relating to the misuse of computer systems since 1985, which means that there are now well-documented cases of misuse. In Britain, there is at present no obligation to report computer misuse. Nor is there any point in doing so because the police are not empowered to do anything about cases in which the computer is the victim, rather than the channel, of the crime. We therefore do not have data about the extent of computer misuse. The only reliable data comes from countries like France, Italy, Sweden, Denmark, Canada, and the United States, where there is legislation relating to computer misuse.

Figure 1 Results of the Butler Cox survey

Nearly a third of the respondents said they had had to forego some business opportunity because of concern over systems security. The commonest lost opportunity was in providing services to travelling staff — services that are increasingly seen as important in meeting customer's requirements for rapid and effective service.

The majority of respondents were aware of incidents of fraud, improper disclosure, sabotage, hacking, or other forms of computer misuse in their organisations. The commonest problem (mentioned by two-thirds of respondents) concerned the misuse of system resources. Much of this misuse was of limited significance (playing computer games, for instance) but it did include the theft of PCs worth £70,000, and obscene and racist material disseminated via bulletin boards.

A quarter of the respondents reported attacks on their computer systems by disgruntled employees, although damage was generally slight. However, the law as it currently stands made it impractical to prosecute those concerned.

A quarter also reported that their systems had been accessed by hackers. Although most respondents believed that this had caused no damage to their systems, one had estimated that the costs of recovering from a major sabotage attack were $4 million. (This estimate was provided for the purpose of obtaining a conviction under US law.)

One in seven of the respondents reported improper disclosure of information held on their computers. Fewer than one in ten were aware of computer frauds, the most costly of which was thefts from ATMs using stolen or forged cards.

Britain has six criminal laws that might, at first sight, be used to deal with hacking. These laws are concerned with forgery, abstraction of electricity, criminal damage, interception of communications, improper use of a public telecommunication system, and data protection. Unfortunately, they are all inappropriate:

- The forgery laws cannot be used because of the decision of the Court of Appeal and the House of Lords in Regina v. Gold and Schifreen. That case was taken to the House of Lords to prove that the forgery concept could not be applied in the context of hacking.
- Abstraction of electricity is an offence against section 13 of the Theft Act. There are technical difficulties in applying this law to hacking, but the major objection to such a charge is its artificiality. The mischief that it seeks to counter is divorced from the substance of the charge — namely, the abstraction of a trivial quantity of electricity.
- Criminal damage laws can be applied only where property has been destroyed or damaged, intentionally or recklessly. The concept of criminal damage does not apply to hacking, even where the data is corrupted.
- The law relating to the interception of communications can be applied only where a hacker intercepts a communication being transmitted by a public telecommunication system. It is seldom an appropriate charge.
- Improper use of a public telecommunication system relates only to sending messages that are offensive. I do not think it even covers bulletin boards.
- The Data Protection Act can apply only if the hacker records personal data that he or she has obtained.

Even the English Law Commission recognises that the existing criminal law is of no real value in the context of computer misuse.

A criminal law is needed

I believe, most strongly, that society cannot expect companies, organisations, and individuals to take large and expensive steps to protect the integrity of their computer systems without providing the appropriate legal backup. I do not pretend that the law can provide for every circumstance, but I contend that society is behaving illogically if, on the one hand, it says to companies and organisations, "You have to lock the door", but on the other hand it says, "By the way, if somebody breaks in we will sit back and do nothing."

I also believe that a civil-law remedy for hacking is inadequate. In my view, the reasoning and recommendations of the Scottish Law Commission report of 1987 should be followed. That report proposed that hacking should be made a criminal offence that could be tried both summarily and on indictment, and be punished by fine or imprisonment, or both. There are many cases known to the police that could have been prosecuted successfully if an anti-hacking law existed.

Many other countries already have laws covering hacking and other computer misuse and it is important that Britain has similar legislation. If we do not, I suggest that we are going to lose a lot of business.

My actions in Parliament

Last year, at the request of the British Computer Society, I sat on the Copyright Bill Committee. We managed to include in the bill several amendments that the software industry thought were crucial. It was wrong that those amendments should have been needed after the Bill had been worked on for 10 years, and it illustrates the gulf of understanding between the legislators and the business world.

The final amendment was a new clause that was designed to prevent hackers from obtaining electronically stored copyright intellectual property. That clause was the spur that persuaded me to try to bring in legislation to outlaw unauthorised actions concerned with computer systems — entry into systems, electronic eavesdropping, data manipulation, data corruption, data addition, and data removal. The legislation would also need to include some allied points, such as making it possible for a machine to be the object of a deception.

Having decided to my own satisfaction that there was a sufficient case for action, I started to work within the parliamentary process. I

wanted to achieve two things. First, I wanted to alert my colleagues on the Government and Opposition benches to this problem. Second, I wanted to try to alert the Government to my concerns, which I believe are industry's concerns, and to brief key Ministers on this problem area.

The Early Day Motion

My first step was to put forward the Early Day Motion shown in Figure 2. (An Early Day Motion is not debated, but MPs can add their names to it to indicate their support.) In wording the motion, I deliberately steered clear of anything that hinted of the right of ownership of information or the value of information. 'Information' is a trigger word in Parliament. Everyone has his or her own preconceived ideas about what 'information' means in the context of government, and any mention of the word will start endless debates. Many in the Labour Party, for example, start from the premise that the full-time aim of the Government is to prevent disclosure of any information at all.

I concentrated on computer hacking because I had discovered through my work on the Copyright Bill Committee that the word 'computer' made many colleagues' eyes glaze over, and caused any Ministers present to retire to the end of the lobby as fast as possible. However, I also discovered that the phrase 'computer hacking' actually attracted their attention. I have therefore deliberately been using the words 'computer hacking' as a sort of trailer. Indeed, the short title of the subsequent Bill I sponsored is the "Anti-Hacking Bill", even though it does not cover the totality of the legislation I was proposing. It certainly does not cover the scope of the legislation the Government should put into its own programme.

Figure 2 The Early Day Motion

Unauthorised penetration of computer files

That this House recognises with the deepest concern, the rash of unauthorised invasions by outside parties of Government and business computer files on mainframe systems; recognises the potential threats to national security posed by such activities as well as other deleterious effects of such breaches of security; urges HM Government to review its current policies on interdiction against offenders and to draft legislation to institutionalise and codify the illegality of these practices and empower the appropriate agencies to step up their efforts at prevention and punishment of future transgressions of this nature.

In all, 42 members have signed the motion to date, including Dr Jeremy Bray, the Opposition spokesman on Science and Technology. I could now seek many more signatures, but there is really no need; it is a cross-party motion and already contains some important names.

Influencing the Government

My next step was to explore the Government's attitude and work. I put forward, I think, 126 Parliamentary Questions to Ministers in February, March, and April. The answers gave no information, but the density and spread of my questions alerted Civil Servants and Ministers across the board to my concerns.

The Anti-Hacking Bill

In May 1989, I introduced a short Private Member's Bill. Such a Bill will become law only if four circumstances co-exist. First, the sponsor needs to draw one of the top six places in the ballot for Private Members' Bills in November (to allow sufficient Parliamentary time.) Second, the Government must want the legislation to be passed. Third, the Opposition must agree with the Government. Finally, the subject matter of the Bill has to be very non-contentious. In the Private Member's Bill system, any MP can stop your Bill, and someone frequently does.

My Bill, had it have been passed, would, subject to certain conditions, have made illegal:

- Unauthorised access to any computer or communications system.
- Radiation eavesdropping and wiretapping.
- Jamming of communications.
- Possession of equipment for use in obtaining unauthorised access.

The penalties prescribed in the Bill include confiscation of equipment, fines, and imprisonment for up to 10 years. The bill also provides certain powers of search and seizure.

My Bill is a perfect example of a Private Member's Bill that not only stood no chance of being passed, but was actually designed so it would not be passed. My purpose was to demonstrate to the Government that a very

short and simple Bill could, in fact, achieve the results required by industry. Another purpose was to have a Bill that I could show to the Prime Minister and other colleagues, as well as send to people who put out all types of scare stories, such as that I was trying outlaw bulletin boards, put a tax on modems, and so on. To show that I did not intend to get it through Parliament, I put the Bill down for debate on 7 July, the last possible Second Reading date for this session. The purpose of the Bill was to stimulate debate and press the Government to act.

The Home Secretary's statement

On the morning of 7 July, Douglas Hurd, the Home Secretary, put out a statement (reproduced in Figure 3) in which he said that the Government was taking a very keen interest in the areas of legislation covered by my Bill, and would be making an early decision. The implication was that the decision would be positive and that the Government might well include such legislation in a forthcoming session. I warmly welcomed this statement and withdrew my Bill.

Figure 3 The Home Secretary's statement of 7 July

"We welcome the valuable work which Emma Nicholson has done in researching this serious problem and bringing it to public attention. The Law Commission are looking into the question of whether the law needs to be changed and, if so, how. They will report by the end of September. We will need to consider their report carefully but quickly in order to decide how best the law can be mobilised to deal with an undoubted mischief."

Since then, I have heard the even more welcome news that such legislation, were it to be introduced, would be sponsored by the Department of Trade and Industry rather than the Home Office. The problem with the Home Office is that it always has too much legislation. Certainly, the Home Office has a very full legislative programme for the next session. Indeed, I believe it is already having to drop some extremely attractive potential pieces of legislation that it just cannot fit in.

In my view, it is wholly right and proper for the Department of Trade and Industry to promote this legislation. Moreover, the DTI has more time to consider it. (The DTI is a member of the Butler Cox Foundation and was represented at the meeting by Mr Casey. The statement he made at the meeting is reproduced in Figure 4.)

Next steps

The English Law Commission published a Working Paper (number 110) in September 1988 on the misuse of computer systems. This Paper called for evidence to be submitted by the end of February 1989. After considerable pressure, this deadline was extended and the Commission has stated that it intends to report at the end of September. This would allow sufficient time for proposed legislation to be included in the Queen's Speech.

However, a report and recommendation by the Law Commission does not necessarily mean that the Government will take action. I have

Figure 4 Comments made by Mr Casey of the DTI

"I am the person in the DTI who will be handling the response to the Law Commission, and my colleague, John Head-Rapson (who is also present), has just joined me to work full-time on that activity.

Our task is to move beyond what Miss Nicholson has done superbly well, and to examine the public case for there being some legislation. There is considerable work to be done in this area, not least because it is not yet clear that all 650 Members of Parliament realise the need for legislation against computer misuse.

In considering our response, one of our main tasks will be to foresee what practical legislation might look like. We therefore have to consider in further detail issues like those raised in the Law Commission's working paper:

- If there is an offence of unauthorised access, what sort of people can authorise access to computer systems?
- If a crime is committed from a location in, say, Scotland, using a telecommunication system that passes over several other countries and accesses a system in the United States, should the courts have jurisdiction?
- Do you define a computer, and, if so, how?

Notwithstanding the Law Commission, we have sought detailed submissions from organisations. We are very keen to talk to people who will be able to make an input on those types of issues because we realise that any legislation will be effective only if we resolve such issues in the right way."

reviewed a list of Law Commission publications going back to 1967 and it is astonishing how many have not been acted on by successive Governments.

In response to suggestions from major computer users and computer-security companies, I am therefore setting up a new and very large group, which I will call something like the 'Computer Misuse Challenge Group', to produce a proper and considered response to the Law Commission report. The first meeting of this group will take place in mid-October.

If the Government then introduces legislation in the shape of a Government Bill, I will reconvene the group and ask it to make recommendations to the Department of Trade and Industry and the Home Secretary. Once the Government Bill has been debated, I will suggest to the group that it monitors the Select Committee process. I believe that this will be the most effective means of harnessing the immense intellectual and practical knowledge of the problems of computer misuse gained by industrial and commercial organisations in recent years.

Appendix: Survey of Foundation members

In order to determine the scale of the problem of improper computer use and the business world's attitude to it, Butler Cox conducted a telephone survey of 42 UK Foundation members. Most Foundation members are large organisations with considerable investments in computer systems. They operate in all business sectors and their views are therefore representative of British businesses as a whole.

The survey examined the business implications of computer security, the frequency and nature of breaches, and the legislation that members would like Parliament to introduce.

Business implications

Twenty-eight per cent of respondents said that at least one new business opportunity or service had been abandoned for computer-security reasons. This was often due to the inability to communicate securely with travelling staff. However, programming computers and communications equipment to dial-out to predetermined numbers was regarded as acceptable by most respondents.

Two respondents had found that the cost of implementing secure dial-out facilities and encryption systems had made it uneconomic to provide commercial services. Two other companies had decided not to offer computer bureau services because of the security implications of hacking.

Most respondents were concerned about the costs and extended implementation timescales associated with the provision and management of sophisticated security systems.

Cost of security

Eighty per cent of respondents were unable to estimate their total computer-security costs. These costs are usually not accounted for separately and are often spread over many cost centres. Where costs could be identified, they varied from one to two per cent of the computing budget in non-finance sectors, up to 20 per cent in one company in the financial sector.

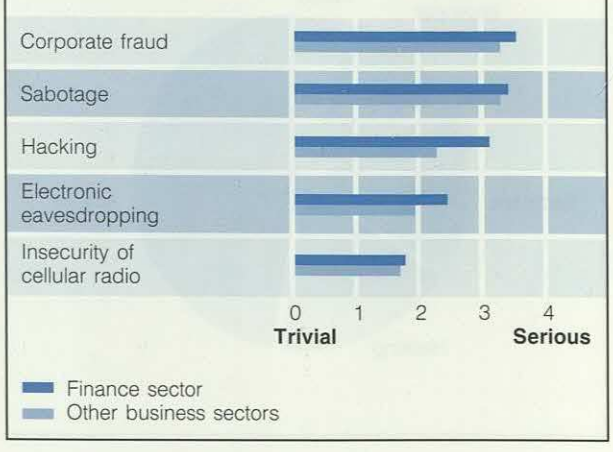
Perceptions of threats

Respondents were asked to rate the seriousness to their businesses of five categories of threat on a scale of one (trivial) to five (serious). The results are shown in Figure 5. Corporate fraud and sabotage were seen as the most serious threats. Non-finance sector organisations perceived hacking to be not a particularly serious threat, although it is a more serious threat to companies in the finance sector. Many of the respondents were not even aware that cellular radio systems could be a threat to security.

Security incidents

Respondents were asked if their organisations had been the victims of breaches of computer security, classified under five categories:

Figure 5 Perceived seriousness of threats to computer security



- Computer-related fraud.
- Sabotage, causing actual damage to hardware, software, or data.
- Improper disclosure, including by penetration of an online system, and by theft of magnetic media or printouts.
- Misuse of computer resources, including playing computer games, unauthorised personal use, resale of time, and theft of property.
- Hacking, defined as unauthorised access to a network or online system.

The results are shown in Figure 6. The most common breach of security was misuse of computer resources, representing 47 per cent of all the breaches reported. Hacking and sabotage were the next most common (19 per cent each). Only 5 per cent of the reported security breaches were computer-related fraud.

Misuse

Most organisations tolerated a limited amount of use of computer systems for personal use, and, until recently, had adopted a similar attitude to computer games. However, the emergence of viruses has caused a significant change in their policies towards computer games and unauthorised software. In many companies, staff can now be sacked if they use computer games or unauthorised software. Most respondents insist that only software delivered in its original 'shrink wrapped' packaging can now be installed. A majority of respondents required any package demonstrations to be given on the supplier's own equipment.

Although not strictly speaking 'misuse', several respondents said that theft was, in the main, restricted to PCs and consumables. One respondent prosecuted an employee who had stolen £70,000 of PC equipment.

Figure 6 Percentage of total incidents by category

Hacking

The respondents who reported unauthorised access attempts on their systems believed that little damage had been caused — except for the sabotage incident described below. More than 50 per cent of the respondents use security software designed specifically to prevent hacking. This type of software reports on failed attempts to enter a system, thus providing early warning of hacking attempts.

Sabotage

Most incidents of sabotage involved disgruntled employees. While dismissals invariably followed sabotage incidents, prosecutions were rare. Often, physical damage was minor and damage to software or databases could not be pursued effectively in the criminal courts. One notable exception concerned a US company that, in the process of prosecuting a hacker, calculated that it had spent $4 million on repairing the damage done to its networked systems.

Improper disclosure

The majority of improper disclosures reported involved internal staff collaboration. One incident of improper disclosure was the transfer of software to a competitor via a diskette. The penalty imposed by the courts reflected the value of the diskette itself, not the value of the information it contained.

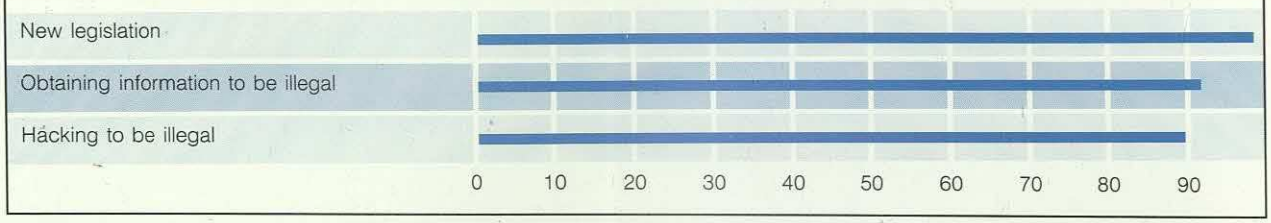
Fraud

Seven per cent of respondents reported computer-related frauds but several suggested that some frauds remained either undetected or were not advised to the computer-security department. A bank reported substantial frauds perpetrated by the use of stolen or forged cards being used in ATMs.

Legislation

As Figure 7 shows, nearly all of the respondents believed there was a need for new legislation.

Figure 7 Percentage of respondents supporting changes to the law



Ninety-eight per cent wanted new legislation to help them combat the threat to computer security. Ninety per cent wanted hacking to be made illegal. Ninety-two per cent said that obtaining and using unauthorised information from a computer system should become illegal. However, many of these perceived that there would be difficulty in drafting legislation that would enable 'information' or 'data' to be treated on the same basis as a tangible asset.

Ten per cent of respondents said that any legislation should allow them to dismiss employees who misuse their computer systems. A similar number suggested that, in the event of a dispute, companies should be called upon to demonstrate that reasonable precautions had been taken to prevent misuse.

Ninety-eight per cent of respondents indicated that they would help to formulate a Butler Cox Foundation response to the report on computer security by the Law Commission of England and Wales.

Bibliography

Flint, David C; Threats to Computer Systems, Foundation Report 51.

Norman, Adrian; Computer Insecurity, 1983. Chapman and Hall.

Parker, Donn; Crime by Computer, 1976. Charles Scribner's Sons.

BUTLER COX FOUNDATION

Butler Cox

Butler Cox is an independent management consultancy and research organisation, specialising in the application of information technology within commerce, government, and industry. The company offers a wide range of services both to suppliers and users of this technology. The Butler Cox Foundation is a service operated by Butler Cox on behalf of subscribing members.

Objectives of the Foundation

The Butler Cox Foundation sets out to study on behalf of subscribing members the opportunities and possible threats arising from developments in the field of information systems.

New developments in technology offer exciting opportunities — and also pose certain threats — for all organisations, whether in industry, commerce, or government. New types of systems, combining computers, telecommunications, and automated office equipment, are becoming not only possible, but also economically feasible.

As a result, any manager who is responsible for introducing new systems is confronted with the crucial question of how best to fit these elements together in ways that are effective, practical, and economic.

While the equipment is becoming cheaper, the reverse is true of people — and this applies both to the people who design systems and those who make use of them. At the same time, human considerations become even more important as people's attitudes towards their working environment change.

These developments raise new questions for the manager of the information systems function as he seeks to determine and achieve the best economic mix from this technology.

Membership of the Foundation

The majority of organisations participating in the Butler Cox Foundation are large organisations seeking to exploit to the full the most recent developments in information systems technology. An important minority of the membership is formed by suppliers of the technology. The membership is international with participants from Australia, Belgium, France, Germany, Italy, the Netherlands, Sweden, Switzerland, the United Kingdom, and elsewhere.

The Foundation research programme

The research programme is planned jointly by Butler Cox and by the member organisations. Each year Butler Cox draws up a short-list of topics that reflects the Foundation's view of the important issues in information systems technology and its application. Member organisations rank the topics according to their own requirements and as a result of this process members' preferences are determined.

Before each research project starts there is a further opportunity for members to influence the direction of the research. A detailed description of the project defining its scope and the issues to be addressed is sent to all members for comment.

The report series

The Foundation publishes six research reports each year. The reports are intended to be read primarily by senior and middle managers who are concerned with the planning of information systems. They are, however, written in a style that makes them suitable to be read both by line managers and functional managers. The reports concentrate on defining key management issues and on offering advice and guidance on how and when to address those issues.

Butler Cox plc
Butler Cox House, 12 Bloomsbury Square,
London WC1A 2LL, England
☎ (01) 831 0101, Telex 8813717 BUTCOX G
Fax (01) 831 6250

Belgium and the Netherlands
Butler Cox BV
Burg Hogguerstraat 791,
1064 EB Amsterdam, The Netherlands
☎ (020) 139955, Fax (020) 131157

France
Butler Cox SARL
Tour Akzo, 164 Rue Ambroise Croizat,
93204 St Denis-Cédex 1, France
☎ (1) 48.20.61.64, Télécopieur (1) 48.20.72.58

Germany (FR)
Butler Cox GmbH
Richard-Wagner-Str. 13, 8000 München 2, West Germany
☎ (089) 5 23 40 01, Fax (089) 5 23 35 15

United States of America
Butler Cox Inc.
150 East 58th Street, New York, NY 10155, USA
☎ (212) 891 8188

Australia and New Zealand
Mr J Cooper
Butler Cox Foundation
Level 10, 70 Pitt Street, Sydney, NSW 2000, Australia
☎ (02) 223 6922, Fax (02) 223 6997

Finland
TT-Innovation Oy
Meritullinkatu 33, SF-00170 Helsinki, Finland
☎ (90) 135 1533, Fax (90) 135 1091

Ireland
SD Consulting
72 Merrion Square, Dublin 2, Ireland
☎ (01) 766088/762501, Telex 31077 EI,
Fax (01) 767945

Italy
RSO Futura Srl
Via Leopardi 1, 20123 Milano, Italy
☎ (02) 720 00 583, Fax (02) 806 800

Scandinavia
Butler Cox Foundation Scandinavia AB
Jungfrudansen 21, Box 4040, 171 04 Solna, Sweden
☎ (08) 730 03 00, Fax (08) 730 15 67