Management Summary

BUTLER COX
FOUNDATION

Systems Security

BUTLER COX FOUNDATION

Systems Security

Management Summary
Report 76, August 1990

Butler Cox plc

LONDON
AMSTERDAM MUNICH PARIS

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

Availability of reports
Members of the Butler Cox Foundation receive three copies of each report upon publication; additional copies and copies of earlier reports may be purchased by members from Butler Cox.

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

Systems Security

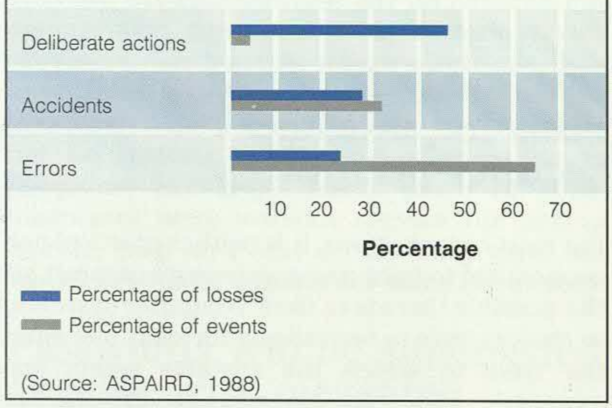
Management Summary

Foundation Report 76, 'Systems Security', was published in August 1990. Its aim is to provide systems directors with a sensible approach to systems security. This document summarises the main management messages arising from our research. The full report is available only to members of the Butler Cox Foundation.

Many managers consider the stories about vast computer frauds, perpetrated by gangs of master criminals or clever juveniles, overplayed and irrelevant to their own business operations. Nevertheless, most would not dispute the fact that threats to systems security are real, and that dealing with them is a complex and demanding task. Figure 1 indicates the scale of the problem.

Figure 1 Deliberate actions are small in number but cause nearly half of the total financial loss

There were 21,000 events involving financial losses and computer systems in France in 1988.



(Source: ASPAIRD, 1988)

Exaggeration by the media does nothing to encourage a rational approach to the subject, but just such an approach is essential if acceptable security is to be achieved at reasonable cost. Absolute security would be extremely expensive and virtually impossible to achieve, however, and would result in a prohibitively restrictive working environment. What is required is an appropriate level of security to meet the organisation's requirements. This Foundation report provides guidance on how that level can be achieved, and draws attention to the implications either of taking action in one area without recognising its broader repercussions, or of failing to take action, and hence, leaving the organisation vulnerable to potential threats.

Security is a management concern

Countermeasures can be taken to prevent threats to computer systems from leading to losses of money, equipment, or information. It is senior management's task to ensure that, taken together, the countermeasures constitute a coherent systems-security policy that provides adequate defences against the threats. A systems-security policy should be developed within the framework of the overall corporate policy for security. Although the board must take the responsibility for ensuring that an overall policy exists, the work of developing and implementing it should be delegated to a small team, possibly headed by a board member, and including technical as well as business expertise. The overall policy should state where attention should be focused, what is expected of individuals and departments, and what means should be employed to achieve the appropriate level of security.

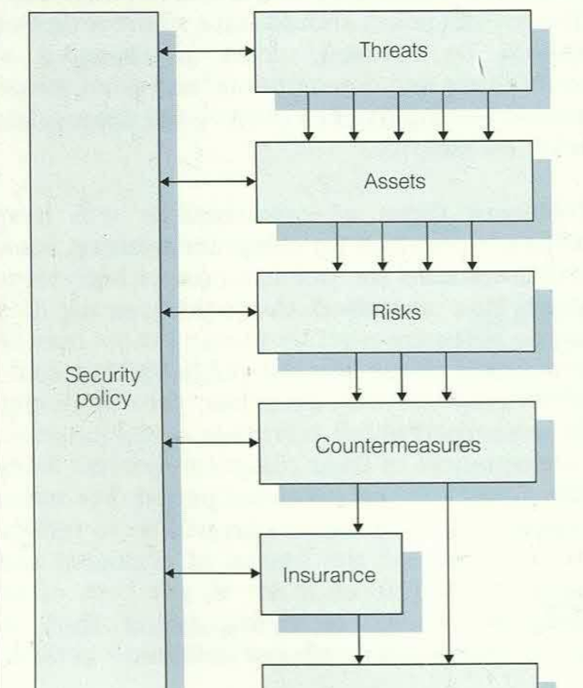
Different types of organisations will have different priorities for computer security. Some will emphasise the need to protect high-value assets (the computers themselves, or the data or the software used by them); others may be concerned about adverse publicity that could result from security breaches; yet others may be concerned about terrorism or the business consequences of their computer systems being unavailable for an extended period. For many organisations, the main aim will be to reduce the number and the impact of accidents and errors, which account for 95 per cent of all systems security incidents, rather than to protect themselves against deliberate actions.

To implement the policy, a security ethic needs to be cultivated so that staff realise the importance, for example, of not leaving terminals logged on when they go home, or not using software of unknown origin. To achieve this, everyone must be fully committed to the concept. Like quality, security is largely an attitude of mind; everyone who has any involvement with the organisation's computer systems must be made aware of their security responsibilities. The development of the detailed systems-security policy is not, however, a one-off activity. The policy should be reviewed and updated at regular intervals (at least every four years) to assess whether it is still effective and to identify any new concerns not covered by the existing policy.

Risk analysis provides the basis for assigning security priorities

For most organisations, it is neither practical nor economical to take countermeasures against all the possible threats to their computer systems, so choices have to be made by formally assessing the risks to which the systems assets are exposed. The risk-assessment process is illustrated in Figure 2. These risks can be listed in order of priority, according to the likelihood of their occurring and the costs that would be incurred.

Figure 2 The relationships between assets, threats, risks, and countermeasures are complex



In carrying out the risk assessments, it is important to look beyond the systems department itself and to consider the way in which IT applications are used by the business. Could the business continue to operate after a fire in a user department, or if there were an industrial dispute that prevented staff from using their terminals?

Technical specialists from within the business and from outside should be involved in assessing the risks, as well as managers with business experience. In some sectors (banking and finance, for example), there are well known independent security experts who can be safely employed. Other organisations could consider using an expert from one of the specialist computer-security groups, such as the 'club' established by the police and computer suppliers in the Netherlands. Otherwise, the wisest course is to choose experts from the organisation's auditors or from reputable consultants, or via trusted industry contacts.

Threats to security may derive from deliberate actions

A major concern is the possibility of threats arising from deliberate actions. Figure 1 showed that, while deliberate actions account for only around 4 per cent of incidents, they account for nearly 50 per cent of financial losses. It therefore pays to have strong protective measures in place, particularly in banks, financial institutions, and large industrial companies, where the heaviest financial losses occur.

Sabotage tends to be most common in periods of social and industrial unrest, and since computer systems are here to stay, they will inevitably become exposed to threats of sabotage at some time. Measures should be set in place to limit the damage that an attack could cause.

To do any damage or to carry out a fraud, however, some form of access is needed. It is estimated that between 70 and 80 per cent of deliberate actions are carried out by insiders, or by those closely associated with the systems attacked. Unless adequate precautions exist, an outsider can readily become an insider, simply by dialling a computer on a data network. Just as strong locks prevent physical entry, strong passwords and other measures can prevent unauthorised access, but because access via a data link is silent, swift, and easily disguised, care is needed to make the 'locks' effective.

A lack of awareness may leave the organisation vulnerable

A certain amount of damage is caused by people making 'positive' mistakes — for example, entering information incorrectly, or deleting information inadvertently. A much greater source of potential errors, however, is 'negative' mistakes caused by human inertia — leaving in place inadequate measures, which themselves create potential risks, or failing to take account of changes in the business environment, and thus leaving the organisation vulnerable to threats that could quite easily be guarded against.

Inadequate countermeasures are a source of potential risk

Most organisations have identified the need to protect their computers from physical threats, like fire and water, and have taken appropriate countermeasures. It is important, however, to check that the protective measures will be effective if a disaster does occur. All too often, damage occurs because the protective measures are not working properly.

It is more difficult to identify threats to data and software. One organisation that thought it had a strong security culture found that, because of the way its operating system was set up, it was possible for one user to amend or delete another user's files, and not be aware that he had done so. This type of 'hole' in computer security is extremely difficult to spot in advance, but is a more frequent source of a breach of security than an attempt to defraud, or to steal data.

Change creates a need for new countermeasures

New threats to computer security arise from the rapid pace of technical advance and the spread of networked computers, both within and between organisations. Many of the well publicised problems with hackers arose because of the creation of computer networks and the lack of awareness of the new risks that they pose.

The increasing penetration of computers into the business also leads to new threats and presents new opportunities for misusing them. Departmental systems, and personal computers in particular, are especially vulnerable to 'software vandals', who wreak their havoc through techniques such as viruses, Trojan horses, and logic bombs (the main report describes how these work, and the countermeasures that can be taken). Personal computers are also easy to steal; an IBM PS/2 fits very neatly into a plastic carrier bag.

The increasing use of, and reliance on, external service providers also creates new threats to systems. Examples include the use of facilities-management companies and network-service providers, particularly where electronic data interchange is involved. Even the risks involved in relying on the public telephone system should not be ignored. When one of the Chicago telephone exchanges burnt down in 1988, businesses were without service for over a month. Such an event is extremely rare, but would be a major disaster for many businesses.

Passwords will be superseded as a security measure

Positive identification of a user logging into a system, rather than of the terminal being used, is one of the keys to ensuring systems security. To date, most organisations have relied on passwords — yet passwords are not, themselves, particularly secure. Passwords can be illicitly acquired, sometimes by simply looking over someone's shoulder or, more often, by guessing that a commonly used password is being used. Figure 3 contains a list of passwords that should be avoided for this reason. Many organisations are therefore seeking an alternative to passwords. The main contenders are authenticators and smartcards for basic security, and biometric sensors for very-high-security systems.

Figure 3 Proper names and commonly used system passwords should not be used as user passwords

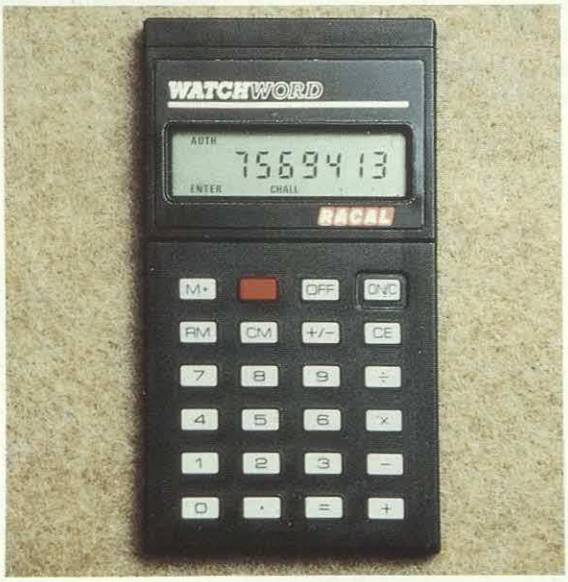
ALEX
BACKUP
DEC
DEFAULT
DEMO
DIGITAL
DOG
FIELD
GUEST
HELP
HIAWATHA
IBM
LAZARUS
NETWORK
MANAGER
OPERATOR
OXFORD
RJE
SERVICE
SYSTEM
TEST
USER
VAX
VMS

Authenticators and smartcards provide good basic security

Authenticators are hand-held, calculator-like devices that hold an encryption-type algorithm (Figure 4 is a photograph of a typical device). After entering his personal identification number (PIN) into a standard terminal, the user simply enters a computer-generated challenge into the authenticator, which calculates and displays the response for the user to key-in to the terminal. If the response matches the computer's expectations, the computer may reasonably conclude that the user is in possession of a valid authenticator. This kind of device is convenient to use, does not require special protocols, and can be used with existing terminals.

Smartcard-based security uses the same basic principle as an authenticator except that much of the processing logic that authenticates the user is carried out by the processor embedded in the card, not by the processor in the hand-held authenticator. Usually, the card contains a secret shared only with the host computer. Once the correct PIN has been entered, the host will ask the smartcard to transmit its secret. The host will know what secret to expect to match up with the PIN. Security can be improved further by basing the dialogue between the smartcard and the host on the concept of zero knowledge systems, which means that the secret itself is not actually transmitted. (The principles of zero knowledge systems are described in the main report.)

Figure 4 Authenticators are calculator-like devices that can be used with existing terminals



Biometric sensors provide absolute authentication

Biometric sensors are used to identify a physical feature of the person trying to access a computer system and to check that it matches pre-stored information about the individual. A wide range of sensors is now available — fingerprint, retinal scans, facial scans, phrenological features, odour, signature analysis, voice print, and typing rhythms. IBM's Transaction Security System, which includes signature-verification facilities, is shown in Figure 5.

The advantage of these methods is that they measure something unique to the individual. It is extremely difficult to fake a fingerprint, retinal image, signature, or facial structure that will deceive a biometric sensor. The main disadvantages are their high cost and, in some cases, social unacceptability. There is also the problem of ensuring that the files of pre-stored information are secure. By definition, these will contain extremely valuable information to someone who wishes to gain unauthorised access to a system. A determined hacker could, in theory, transmit a stream of data that will lead the checking software to believe that it has received a valid input from a biometric sensor.

Figure 5 IBM's Transaction Security System includes signature-verification facilities

The pen measures the acceleration and pressure applied by the user, and compares the values with stored values in the Personal Security (TM)* card. The stored values are updated with the values derived from the last verified signature, so that slight trends in signature patterns over time can be catered for.

*(TM) Trademark of the International Business Machines Corporation

Better access controls will reinforce systems security

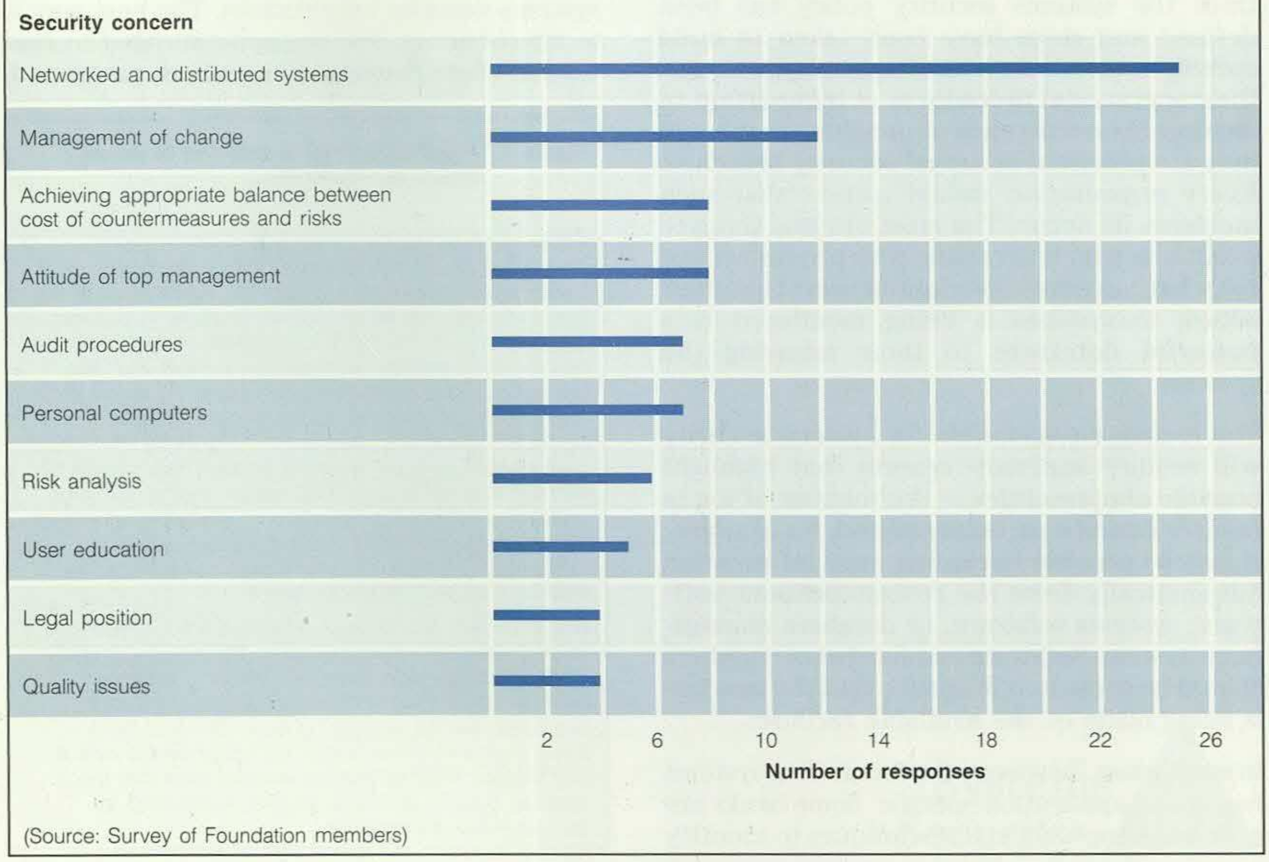
Access control is not just about which passwords do or do not allow access to the system; it is also about who has access to what parts of the system and what data they may access and update. In a simple computing environment, today's access-control software packages can work satisfactorily, but when the computing environment begins to get more complex, simple access controls begin to fail. Indeed, the security implications of networked computer systems are a major concern for Foundation members, as Figure 6 illustrates. What is needed is better access-control software. Access control and security considerations go right to the heart of computer operating-system design and therefore have an impact not only on technical but also on commercial considerations. Better access-control software is becoming available for a restricted range of multivendor environments and the situation is improving within single-vendor software environments. The developments in the most widely used packages are described in the main report.

Built-in integrity checks will automatically detect many security breaches

If integrity checks are designed into systems at the start, built-in checks and balances will help to ensure that errors, as well as frauds, are automatically prevented. Some integrity is assured by the introduction of routines that check the internal consistency of data. This is a normal design technique that, at least, ensures that 'the books balance'. Closely allied to this technique is the concept of the 'well formed transaction', an accounting principle that should be embodied in application programs and audit trails. In essence, it, too, ensures that the books balance. For every debit entry, there is a corresponding credit entry, and it is never possible to access one entry without affecting the other.

The corruption of existing programs and data can be largely prevented by strong physical protection and by encrypted digital signatures. There is, however, little that can be done to

Figure 6 The security implications of networked and distributed computer systems are a major concern for Foundation members



(Source: Survey of Foundation members)

prevent a determined programmer from introducing a Trojan horse or a logic bomb into a program at the design or coding stage. Structured walkthroughs and inspections will find most of the problems, but as with any manual method, there is always a chance that some will escape detection.

Although they are an essential feature of systems security, technical countermeasures will do little to prevent dishonesty. The 'division of duties' principle is often used to ensure that the computer is not deceived by a single individual. Of course, collusion between individuals can subvert this principle, but other measures, such as the periodic rotation of duties among individuals, will restrict opportunities for collusion. Division of duties is fundamental to the preservation of information integrity, and must be maintained, regardless of local difficulties, or broader organisational problems. Where a shortage of staff or the business structure make it difficult to apply the principle locally, it may be necessary to use information technology to separate the duties geographically.

Potential security breaches should be monitored

Once the systems security policy has been defined and steps have been taken to build security measures into the design of systems and their operational procedures, it is important to monitor the occurrence of incidents that could indicate potential or actual security breaches. Every organisation should assume that such incidents do occur. The most obvious thing to monitor is who is accessing which systems, and for what purposes. Reminding users that their access to systems is being monitored is a powerful deterrent to their misusing the systems.

The manager responsible for systems security will require summary reports that highlight possible abnormalities — the number of log-in failures during a particular period, for example. It may be possible to capture such information automatically from the communications software, systems software, or database management system. Software and hardware suppliers should be consulted to ensure that the best use is being made of the available facilities.

In some cases, however, the monitoring systems have to be application-specific. Some banks are now using sophisticated techniques to identify possible fraud attempts involving automatic teller machines (ATMs). Unusual patterns of cash withdrawal from ATMs can be detected and the ATM network closed down.

Research, particularly in the United States, has led to the use of expert-system techniques to detect anomalies (and therefore potential security breaches) in the use of computer systems. One such development is described in Figure 7, and illustrates the type of technique that will eventually find its way into commercial products.

It pays to have contingency plans in place

The process of recovering from a hardware breakdown or a software fault may, itself, represent a potential security threat, particularly for major computer installations in the finance industry. The whole purpose of recovery is to get back to a fully operational system as quickly as possible. Computers are vulnerable during the recovery process — albeit for a short time, thereby creating opportunities for security to be compromised.

Contingency and recovery plans of all types should therefore be reviewed to assess their systems-security implications. The best way is to try them out. We were discouraged to find that, of those Foundation members questioned,

Figure 7 The IDES system is designed to detect threats automatically

IDES (Intrusion Detection Expert System) is being developed at SRI International's Computer Science Laboratory in Menlo Park, California, funded by the US Navy's Space and Naval Warfare Systems Command. The system runs on two Sun workstations and is based on Oracle's database management system and SQL. No *a priori* rules are built into the system; instead, it 'learns' the behaviour of each user and detects significant changes in behaviour. It works by monitoring such factors as log-in time and location, the amount of connect time, CPU time, input/output usage, and any protection violations. Log-in time is divided into three parts — day, evening, and night/weekends/public holidays. The violations reported on include directory modifications and password errors.

This approach is unreliable, however, if it is introduced when people are already abusing the system, because IDES will simply learn their bad habits. Furthermore, because IDES maintains profiles of user behaviour averaged over 50 days, it could be defeated by a clever user who slowly varies his usage profile over a long period. Whether system abusers have that much patience is open to doubt. Work is proceeding to address these weaknesses.

only 50 per cent exercised their contingency plans fully, on a regular basis, and three-quarters of these admitted that their first attempt had failed, or that the plan had been defective.

Contingency plans should also include instructions on what to do in the event of a breach in computer security being discovered. It is surprising how often a computer fraud is discovered late in the afternoon on the day before a public holiday, or at a time when managers are not available to authorise drastic action.

In summary, guidelines for a good systems security policy are similar to those for a quality-management policy:

— Establish a security ethic.

— Design security into computer systems and applications.

— Establish controls to identify possible problems as early as possible.

— Establish controls that are appropriate to the severity of the threats.

— Do not over-control; install the simplest, most efficient, and most economical solution.

— Do not delay improvements by over-analysis.

— Record the threats identified, the risks resulting from those threats, and the countermeasures taken.

Full details can be found in the main report.

BUTLER COX
FOUNDATION

The Butler Cox Foundation

The Butler Cox Foundation is a service for senior managers responsible for information management in major enterprises. It provides insight and guidance to help them to manage information systems and technology more effectively for the benefit of their organisations.

The Foundation carries out a programme of syndicated research that focuses on the business implications of information systems, and on the management of the information systems function, rather than on the technology itself. It distributes a range of publications to its members that includes Research Reports, Management Summaries, Directors' Briefings, and Position Papers. It also arranges events at which members can meet and exchange views, such as conferences, management briefings, research reviews, study tours, and specialist forums.

Membership of the Foundation

The Foundation is the world's leading programme of its type. The majority of subscribers are large organisations seeking to exploit to the full the most recent developments in information technology. The membership is international, with more than 400 organisations from over 20 countries, drawn from all sectors of commerce, industry, and government. This gives the Foundation a unique capability to identify and communicate 'best practice' between industry sectors, between countries, and between IT suppliers and users.

Benefits of membership

The list of members establishes the Foundation as the largest and most prestigious 'club' for systems managers anywhere in the world. Members have commented on the following benefits:

— The publications are terse, thought-provoking, informative, and easy to read. They deliver a lot of message in a minimum of precious reading time.

— The events combine access to the world's leading thinkers and practitioners with the opportunity to meet and exchange views with professional counterparts from different industries and countries.

— The Foundation represents a network of systems practitioners, with the power to connect individuals with common concerns.

Combined with the manager's own creativity and business knowledge, Foundation membership contributes to managerial success.

Recent Research Reports

57 Using System Development Methods
58 Senior Management IT Education
59 Electronic Data Interchange
60 Expert Systems in Business
61 Competitive-Edge Applications: Myths and Reality
62 Communications Infrastructure for Buildings
63 The Future of the Personal Workstation
64 Managing the Evolution of Corporate Databases
65 Network Management
66 Marketing the Systems Department
67 Computer-Aided Software Engineering (CASE)
68 Mobile Communications
69 Software Strategy
70 Electronic Document Management
71 Staffing the Systems Function
72 Managing Multivendor Environments
73 Emerging Technologies: Annual Review for Managers
74 The Future of System Development Tools
75 Getting Value from Information Technology
76 Systems Security

Recent Position Papers and Directors' Briefings

Information Technology and Realpolitik
The Changing Information Industry: An Investment Banker's View
A Progress Report on New Technologies
Hypertext
1992: An Avoidable Crisis
Managing Information Systems in a Decentralised Business
Pan-European Communications: Threats and Opportunities
Information Centres in the 1990s
Open Systems

Forthcoming Research Reports

New Telecommunications Services
The Role of IT in Transforming the Organisation
Electronic Marketplaces
Managing the Distribution of IT
The Future of Electronic Mail

Butler Cox

The Butler Cox Foundation is one of the services provided by the Butler Cox Group. Butler Cox is an independent international consulting company specialising in areas relating to information technology. Its services include management consulting, applied research, and education.

BUTLER COX FOUNDATION

Butler Cox plc
Butler Cox House, 12 Bloomsbury Square,
London WC1A 2LL, England
☎ (071) 831 0101, Telex 8813717 BUTCOX G
Fax (071) 831 6250

Belgium and the Netherlands
Butler Cox Benelux bv
Prins Hendriklaan 52,
1075 BE Amsterdam, The Netherlands
☎ (020) 75 51 11, Fax (020) 75 53 31

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

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 2985

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

Spain and Portugal
T Network SA
Núñez Morgado 3-6°b, 28036 Madrid, Spain
☎ (91) 733 9866, Fax (91) 733 9910