Chapter 1

OPPORTUNITIES FOR LEARNING

Introduction

Millions of pounds are wasted on information system projects that fail and millions more are lost due to malfunctions of systems that have progressed beyond the implementation stage. The horror stories are easy to find, at least where large projects in the public sector are concerned. For example:

- In 1996 the Integrated Justice Project was set up in Ontario, Canada, with the aim of building an information system for Ontario's entire justice sector. In March 1998 the investment required was estimated to be $180 million and the benefits as $326 million. By March 2001 the figures had become an investment of $312 (of which $159 million had already been spent) and benefits of $238. Thus the benefit–investment ratio had changed from 1.81 : 1 to 0.76 : 1.
- Also in 1996 the Benefits Agency of the UK government's Department of Social Security and Post Office Counters Ltd awarded a contract to Pathway, a subsidiary of the ICL computer services group, to provide recipients of social security benefits with magnetic stripe payment cards. The project was abandoned exactly three years later. The National Audit Office estimated that the cancellation cost over £1 billion.
- In 1998 The Lord Chancellor's Department commissioned 'Libra', a system to support the work of magistrates' courts in England and Wales. By 2002 the cost of the project had doubled to almost £400 million but the scope had reduced drastically.
- In 1999 delays in processing British passport applications, following the introduction of the Passport Agency's new system, cost £12 million including, it is alleged, £16 000 spent on umbrellas to shelter those queuing in the rain to collect their passports.
- In 2002 a project to replace the British Army, Royal Navy and Royal Air Force inventory systems with a single system (the Defence Stores Management Solution) was brought to a halt after £130 million had been spent. Hardware worth a little over £12 million was able to be used elsewhere but the remaining £118 million was written off as a loss.

- In 2003 it was revealed that the British government had to pay over £2 million extra to its contractor, Capita, following a big increase in the number of applications for criminal records checks being made in writing instead of by telephone or electronically. This was just one of a series of adverse reports involving the Criminal Records Bureau. Some schools had to delay the start of the autumn term due to backlogs in the processing of teachers' applications, and at the start of November inquiries into the background of care workers in charge of children and the elderly were suspended for a period of up to 21 months in order to ease the pressure on the system.

Not all failures can be expressed in financial terms. On 19 January 1982, following the Byford Report on an inquiry into what had gone wrong with West Yorkshire Police's hunt for the serial killer dubbed 'The Yorkshire Ripper', the then Secretary of State for the Home Department, William Whitelaw, said to the House of Commons:

> Another serious handicap to the investigation was the ineffectiveness of the major incident room which became overloaded with unprocessed information. With hindsight, it is now clear that if these errors and inefficiencies had not occurred, Sutcliffe would have been identified as a prime suspect sooner than he was.

There seems to be widespread agreement that this identification could have occurred at least a full 18 months sooner. In those 18 months, another three women were murdered.

By 2004 police forces were still experiencing information system failures. A Public Inquiry report on child protection procedures in Humberside Police and Cambridgeshire Constabulary (Bichard, 2004) found:

> The process of creating records on their [Humberside Police's] main local intelligence system – called CIS Nominals – was fundamentally flawed … Police Officers at various levels were alarmingly ignorant of how records were created and how the system worked. The guidance and training available were inadequate and this fed the confusion which surrounded the review and deletion of records once they had been created.
>
> The failures in the use of CIS Nominals were compounded by the fact that other systems were also not being operated properly. Information was not recorded correctly onto the separate CIS Crime system. It took four years

> (from 1999 to 2003) for those carrying out vetting checks to be told that the CIS 2 system, introduced in late 1999, also allowed them to check a name through the CIS Crime system.
>
> (Bichard, 2004, p. 2)

The private sector also has its share of failures, although they tend to be smaller in scale and are often hidden behind closed doors. Nevertheless, examples do emerge into the public gaze:

- On 25 February 2000 at the High Court, Queens Bench Division, Technology and Construction Court, Wang (UK) Limited was ordered to pay damages of a little over £9 million to Pegler Ltd, a Doncaster-based engineering firm. Wang had entered into a contract to supply Pegler with a bespoke computer system to process sales, despatch, accounts and manufacturing systems and associated project management and consultancy services. Six years after the contract was signed it was formally terminated by Pegler but, in effect, it had been abandoned by Wang before that. Wang claimed that exclusion causes in the contract meant that it was not liable for damages, but the court found against it and it had to pay compensation for lost opportunities, wasted management time and reduced business efficiency and recompense Pegler for money it had spent elsewhere on outsourcing and software acquisition.
- In 2002 in the USA, the pharmaceutical company Eli Lilly settled out of court with the Federal Trade Commission after being accused of violating its own online privacy policy by revealing the e-mail addresses of 669 patients who were taking the antidepressant drug, Prozac.
- Also in 2002 the Dutch Quest division of ICI, which makes fragrances for perfume manufacturers, lost an estimated £14 million as a result of problems with its new SAP enterprise resource management system.
- At the start of 2003, the first stage of a legal battle to recover £11 million was fought by the Co-operative Group against Fujitsu Services (formerly ICL). The case concerned alleged shortcomings in a programme to install a common IT infrastructure across the whole of the Co-operative Group following the merger between the Co-operative Wholesale Society (CWS) and the Co-operative Retail Services (CRS). A significant aspect of the problem was the system needed to spread CWS's dividend loyalty card across all the Group's stores.
- In May 2003, Energywatch, the independent gas and electricity consumer watchdog set up by the Utilities Act (2000), published information claiming that billing

problems had affected 500 000 gas and electricity consumers over the previous 12 months. Research conducted on their behalf by NOP World suggested that 9% of consumers had experienced debt due to estimated billing. The cost to consumers was stated to be £2 million in avoidable debt. It was also estimated that almost 50 000 British Gas customers throughout the UK do not receive their first bill for up to a year and, as a consequence, owe British Gas around £13 million. In 1999 British Gas served a writ on systems supplier SCT International claiming damages in respect of software it had supplied for billing business gas customers.

Examples such as these lie at or near the pinnacle of a mountain of failure. Beneath lies examples such as the incident in Japan on 1 March 2003 when failure of the system that transmits such data as flight numbers and flight plans to airports led to the cancellation of 122 flights and delays to a further 721. On the lowest slopes are the failures we all experience on a regular basis such as the long queue at the library while the numbers of the borrowers and their books are written out by hand because the system is down again and the delay at the supermarket checkout because a price is missing on the point of sale system. Obviously, not every coding error or design snag or glitch in the operation of an information system merits serious investigation, but even when these failures are excluded there are still ample left to study.

Opportunity for learning

In wondering what can be done about such failures, two things are indisputable: first, some failures will always occur and, second, the vast majority are avoidable. The reasons why they are not avoided are manifold, but a major reason is the inability to learn from mistakes. A survey by Ewusi-Mensah and Przasnyski (1995) provides one explanation of this lack of learning. In an attempt to discover the kind of post-mortem appraisals that had been carried out, they conducted a survey of companies that had abandoned information system (IS) development projects. Their findings suggested 'that most organizations do not keep records of their failed projects and do not make any formal efforts to understand what went wrong or attempt to learn from their failed projects' (p. 3).

Emergency planning has tended to be the norm in many high-risk technologies, such as nuclear power generation and oil production, and the number of commercial organizations making similar plans is increasing, especially since the attacks on the World Trade Center in New York in 2001. However, there are still a significant number

who seem to be remarkably reluctant to anticipate that things might go wrong with their information systems. A Global Information Security Survey of 1400 organizations in 66 countries conducted by Ernst & Young in 2003 found that over 34% of those surveyed felt themselves to be 'less than adequate' at determining whether or not their systems were currently under attack, and over 33% felt that they were 'inadequate' in their ability to respond to incidents. A similar survey of the world's biggest companies, conducted by market analyst Meta Research in the same year, found that only 60% had 'a credible disaster recovery plan that is up-to-date, tested and executable'. The picture is unlikely to be rosier where smaller organizations are concerned.

One of the features of information systems that renders them prone to failure is the very high extent to which they need to be embedded in the organizations using them. As Walsham (1993, p. 223) says:

> The technical implementation of computer-based IS is clearly necessary, but is not sufficient to ensure organizational implementation with respect to such aspects as high levels of organizational use or positive perceptions by stakeholder groups. Organizational implementation involves a *process of social change* over the whole time extending from the system's initial conceptualization through to technical implementation and the post-implementation period.

Given this need to take account of the organizational setting of an IS, learning at the level of the organization is likely to be particularly important.

Organizational learning

Argyris and Schon, the founding fathers of the concept of organizational learning, began their first major book on the topic with a story about failure:

> Several years ago the top management of a multibillion dollar corporation decided that Product X was a failure and should be disbanded. The losses involved exceeded one hundred million dollars. At least five people knew that Product X was a failure six years before the decision was taken to stop producing it. . . .
>
> (Argyris & Schon, 1978, p. 1)

They then examined why production had continued for so long, and concluded:

> Difficulties with and barriers to organizational learning arose as it became clear that the original decision (and hence the planning and problem solving that led to the decision) was wrong. Questioning the original decision violated a set of nested organizational norms. The first norm was that policies and objectives, especially those that top management was excited about, should not be confronted openly. The second norm was that bad news in memos to the top had to be offset by good news. (p. 3)

Similar scenarios, where organizations continue with a system that is not delivering, are by no means rare in the information system domain.

The main thrust of Argyris and Schon's argument is that organizational learning involves the detection and correction of error. They draw a distinction between two types of learning: single loop and double loop.

> When the error detected and corrected permits the organization to carry on its present policies or achieve its present objectives, then that error-detection-and-correction process is *single-loop* learning. Single-loop learning is like a thermostat that learns when it is too hot or too cold and turns the heat on or off. The thermostat can perform this task because it can receive information (the temperature of the room) and take corrective action. *Double-loop* learning occurs when error is detected and corrected in ways that involve the modification of an organization's underlying norms, policies, and objectives. (pp. 2–3)

They emphasize that both types of learning are required by all organizations, and in a later work Argyris (1992, p. 9) provides guidance on the use of each:

> Single-loop learning is appropriate for the routine, repetitive issue – it helps to get the everyday job done. Double-loop learning is more relevant for the complex non-programmable issues – it assures that there will be another day in the future of the organization.

It is Argyris and Schon's assertion that 'organizations tend to create learning systems that inhibit double-loop learning' (p. 4).

The work of Argyris and Schon emphasizes the learning process. Senge (1990) gives it a stronger practical focus by identifying the following five disciplines, or bodies of theory and technique, which, when brought together, create the capacity to learn:

1. *Systems thinking* – which integrates the other four disciplines. For Senge this is concerned with seeing developing patterns rather than snapshots. 'At the heart of the learning organization is a shift of mind – from seeing ourselves as separate from the world to being connected to the world, from seeing problems caused by someone or something "out there" to seeing how our own actions create the problems we experience.'
2. *Personal mastery* – a personal commitment to lifelong learning by individuals in the organization. Mastery is seen in the craft sense of constantly striving to improve on the personal skills that the individual has acquired.
3. *Mental models* – Senge argues that there are deeply ingrained assumptions and images that influence both the way individuals perceive the world and the actions that are taken. These mental models are different from the 'espoused theories' in that they are based on observed behaviour. In Senge's view, these models need to be brought into the open so that they can be subjected to scrutiny.
4. *Building shared vision* – Senge posits that if organizations are to be successful everyone must pull in the same direction towards the same vision of the future – and they must do that because they want to, not because they are told to. 'You don't get people to buy into a vision, you get them to enrol.' The commitment to learning is a part of that vision.
5. *Team learning* – the team rather than the individual is the key learning unit in most views of a learning organization. Primarily this is because a team is regarded as a microcosm of a whole organization, but it may also be influenced by the knowledge that there was already a body of established management literature on the creation of successful teams.

As can be seen from the above, much of the thrust of Senge's approach is linked to the idea of human-centred management; it is about allowing the individuals throughout an organization to contribute fully to its future development, and about making sure that senior management discharge their responsibilities for ensuring that strategy is clearly articulated and that staff are nurtured.

In a paper published in 1991, Huber sets out four constructs that he regards as integrally linked to organizational learning. These are: knowledge acquisition; information distribution; information interpretation; and decision-making. Argyris and Schon's work

has been criticized (see Sun & Scott, 2003, p. 205) for not addressing 'the triggers that spur the learning process'. In his unpicking of knowledge acquisition, Huber goes some way towards addressing this. He identifies five processes through which organizations can obtain knowledge:

1. *Congenital learning* This involves taking on board the knowledge inherited at the conception of the organization and the additional knowledge acquired prior to its birth.
2. *Experiential learning* This can be achieved in a number of ways and can even be unintentional.
3. *Vicarious learning* This is the acquisition of second-hand experience from other, often competing, organizations and is often accomplished by imitation.
4. *Grafting* Knowledge is acquired by recruiting new members with the desired knowledge, sometimes to the extent of taking over a complete organization.
5. *Searching and noticing* This can take three forms: scanning the environment; focused search; and monitoring of the organization's performance.

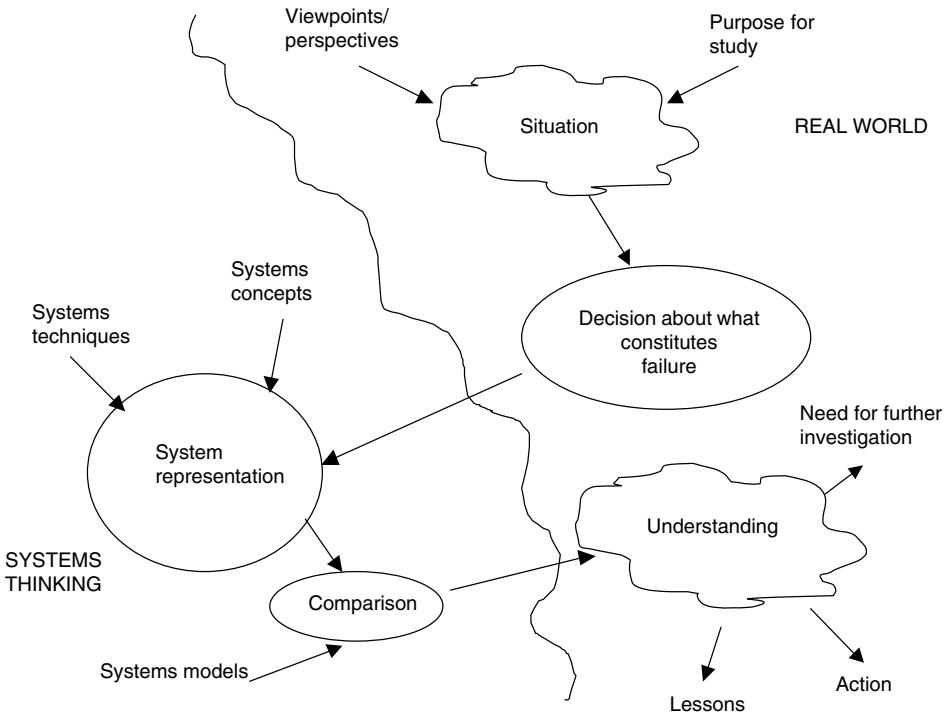

Figure 1.1 A notional view of the Systems Failures Approach

However, as Sun and Scott (2003, pp. 206–207) point out, both Huber and Senge concentrate on explicit knowledge and thereby fail to consider tacit knowledge to a sufficient extent. One of the advantages of the Systems Failures Approach is that it can develop tacit knowledge to the point where it can be replicated. As with other systems approaches, such as Soft Systems Analysis (SSA) and Total Systems Intervention (TSI), the Systems Failures Approach takes the analyst from the real world (in this case the situation labelled as a failure or a potential failure) into the conceptual world where systems thinking, qualitative modelling and comparison provide the means by which understanding can be achieved. This understanding is then taken back to the real world, where it emerges as a set of lessons that can be shared. This journey is illustrated in Figure 1.1.

Beyond the organization

Although they sometimes appear startlingly reluctant to do so, organizations can also learn from one another, and in the field of IS development it is very important that they should do so, even where a single organization might only undertake a large project once in a blue moon.

A major source of lessons that is widely available is in public administration and governance. In the UK a long series of high-profile and very costly failures led the Committee on Public Accounts to investigate 'more than 25 cases from the 1990s where the implementation of IT systems has resulted in delay, confusion and inconvenience to the citizen and, in many cases, poor value for money to the taxpayer' (Committee of Public Accounts, 1999). Every one of the cases they looked at was an IS project. As a result of this investigation, and additional criticism from the National Audit Office, a major review of government IT projects was commissioned by the Prime Minister. Its findings were published by the Cabinet Office in May 2000 in a report (Cabinet Office, 2000) that sets out measures to improve project delivery and includes 30 recommendations that aim to ensure that all government IT projects are as good as the best.

Before leaving the topic of learning from one another, it is worth asking the question: 'Are IS failures different from other failures?' This book deals specifically with information system failures but the Systems Failures Approach is equally applicable to all sorts of complex failure situations from natural disasters, transport accidents, construction projects, company collapses, large-scale frauds, etc. Although it is debatable whether IS failures are different, they certainly have many features in common with those

experienced elsewhere, as you will see in the following chapter where we look at the characteristics of failure.

Overview of the book

The aim of this book is to promote learning by providing a general understanding of the nature of failure and a systems approach (the Systems Failures Approach) by which it can be analysed, understood and predicted. The main argument is that through the use of systems thinking it is possible to gain insights into failure that would not otherwise be available. The book also introduces a variety of methods and techniques that have been developed by others, and thus allows the reader to see them alongside the Systems Failures Approach put forward by the authors. The emphasis here is on taking learning beyond direct personal experience to a level that encompasses learning from situations in which one played no part, and of which one might have had no direct experience.

Chapter 2 looks at the nature of success and failure and at ways in which IS failures can be classified. It explores the stages of the IS life cycle to identify points where things may go awry.

Chapter 3 tells the story of two projects. At the outset the projects seemed to be very similar and equally likely to succeed. They were about the same size and scope and the organizations in which they were being undertaken had many features in common. In the event, however, the two projects could not have been more different in one extremely important respect: one was largely successful across the whole of the range of measures normally used to judge success; but the other exhibited most of the characteristics of failure.

Chapter 4 introduces a range of systems concepts and shows how their use can lead to an understanding of a failure situation. Among the concepts covered are: appreciative system, holism, environment, boundary, hierarchy, control and communication.

Chapter 5 is another case study. It is based on two reports commissioned by Cambridge University into the development of an online commitment accounting software system. The project attracted widespread bad publicity for the University with headlines pointing to the waste of £10 million. Worse still, the system continued to cause disruption to the University's activities long after it was installed, and led to calls to examine the way the University is governed. This case, together with those in

Chapter 3, provides examples for Chapters 6 and 7, which look at how the Systems Failures Approach works. It also provides source material with which others can conduct their own analyses.

Chapters 8 and 9 are also built around case studies. Chapter 8 looks at two of the examples mentioned at the beginning of the chapter: the Benefits Payment Card project that was abandoned after three years, and Project Libra, the magistrates' court information system. In Chapter 9 the direction of the analysis changes from looking backwards to looking forwards. The main purpose of Chapter 9 is to illustrate the process of using the Systems Failures Approach to prevent failure. It reports a study that was commissioned by the Department of Health as it embarked upon a large-scale IS project to design, develop and implement electronic patient records. The study was in two parts: first, published accounts (mainly American and Canadian) of attempts to introduce clinical information systems were analysed; then the findings of the first stage, together with lessons from other large-scale IS projects and information gained from interviews with interested parties, were used to look forward to the development and introduction of the National Health Service's new system with a view to predicting the system's associated risks.

Chapter 10 examines various approaches that different authors have taken to understand, explain, intervene in and prevent failures. The chapter begins with project management approaches relevant to IS failures. It then moves on to discuss general approaches to failure and specific approaches developed to understand IS failures. It ends by returning to the Systems Failures Approach.

Throughout this book the emphasis will tend to be on practical application, with the theory that underpins the work being brought in to explain what is being undertaken, and why. Case studies are used as the vehicle for introducing the Systems Failures Approach and for demonstrating it in action, with further case study material being supplied to enable the reader to try out the ideas, techniques and procedures.

References

Argyris, C. (1992) *On Organizational Learning*. Blackwell, Oxford.

Argyris, C. & Schon, D.A. (1978) *Organizational Learning: A Theory of Action Perspective*. Addison-Wesley, Reading, MA.

Bichard, M. (2004) *The Bichard Inquiry Report*. The Stationery Office, London.

Cabinet Office (2000) *Successful IT: Modernising Government in Action*. Cabinet Office.

Committee of Public Accounts (1999) *Improving the Delivery of Government IT Projects*. Committee of Public Accounts.

Ernst & Young (2003) *Global Information Security Survey*. Ernst & Young.

Ewusi-Mensah, K. & Przasnyski, Z.H. (1995) Learning from abandoned information development projects. *Journal of Information Technology*, 10: 3–14.

Huber, G.P. (1991) Organizational learning: The contributing processes and the literatures. *Organization Science*, 2: 88–115.

Senge, P.M. (1990) The leader's new work: Building learning organizations. *Sloan Management Review*, 7–23.

Sun, P.Y.T. & Scott, J.L. (2003) Exploring the divide – organizational learning and learning organization. *The Learning Organization*, 10: 202–215.

Walsham, G. (1993) *Interpreting Information Systems in Organizations*. John Wiley & Sons, Chichester.