# Information Systems Failures: Can we make professionals more responsible?[1]

Elli Georgiadou and Carlisle George

School of Computing Science, Middlesex University,
London, United Kingdom
Email: e.georgiadou@mdx.ac.uk, c.george@mdx.ac.uk

**Abstract**

Information Systems (IS) fail with alarming regularity despite the many efforts by the Software Engineering community over the last 40 years to understand and to minimise failures. The impact of Information Systems failure results in financial losses but more importantly in loss of life. As modern society depends increasingly on Information and Communication technologies it is imperative that systems are reliable, accurate, timely and cost-effective. These qualities are often recognised by their absence. When things go wrong it is normal to look for the causes of failure but it is also necessary to identify who is responsible. Apportioning blame and responsibility has become a norm, and the culture of litigation has been permeating many societies in the past decades. It is therefore surprising that no one was found personally responsible (liable) for past failures of some safety critical systems (London Ambulance Disaster) or systems leading to huge financial loss (Arianne 5, Tokyo Stock Exchange). This is of concern, especially if future IS professionals become insensitive to failure, and if they develop a culture of not taking personal responsibility for their actions. In this paper we explore some of the main reasons for systems and project failures, reported by researchers and practitioners with the view to contributing to the discussions surrounding the need for professional responsibility. We discuss the concept of responsibility in a legal context, examining how the law is applied to establish liability for one's behaviour. We argue that the increasing importance of IS professionals may merit the need for regulatory bodies similar to what obtains for some established professions like medicine and law. We further discuss the difficulty of applying such regulatory mechanisms to IS professionals. Finally, we conclude that the need for IS professionals to become more responsible and accountable to society, as IS plays an increasingly critical role in our lives, may justify IS professional regulatory bodies in the future.

---

[1] Georgiadou, E. and George, C. (2006), Information Systems Failures: Can we make professionals more responsible? In R Dawson, E Georgiadou, P Linecar, M Ross and S Staples (Eds), *Software Quality Management XIV, Perspectives in Software Quality, Proceedings of the 14th International Software Quality Management (SQM) conference*, 10-12th April 2006, Southampton Solent University, Southampton UK, (British Computer Society), pp 257-266.

# 1.0 Introduction

Failures and successes of Information Technology (IT)/Information Systems(IS) projects have been discussed since the early 70s when organisations started to use computer technology to harness the ability of their information systems [1]. IT project failures have been studied and presented by numerous researchers [2,3,4,5]. The statistics available [6,7] show that a high proportion of IT projects fail in some way. Failures range from total malfunction, break-down, abandonment, rejection or non-use.

In many cases similar factors of failure have been cited in different projects. These include schedule overrun; timescale overrun; lack of management involvement and lack of user involvement [8,9].

"What is meant by a 'quality system'? The answer depends on who is answering the question. While a software system is being developed, and during its use, there are different categories of people to whom good quality software is important. Systems have a multiplicity of people involved throughout their lifecycle. Systems are developed and they have a life, they evolve, adapt and die, hence we use many 'words to describe' them, which are relevant to the various stakeholders namely end-users, developers and sponsors. Availability, reliability, correctness, usability, expandability, maintainability span the views and expectations of a range of people involved [10,11].

In studying IS project failures for over three decades, [1] presented their findings and pointed out the complexity of IS projects. They presented an IS failure classification framework with different domains where they believed failure can occur (technical, data, user and organisation). These four domains represent stakeholder groups in an organisation. With this, they define IS failure as the "inability of information systems to meet stakeholder group's expectation". Safety critical systems are expected to possess very high reliability due to the use of formal specification and formal testing.

Donaldson and Jenkins [12] observe that "The causes of systems and project failures, vary considerably. Each case has to be taken in isolation and examined, to see where it has gone wrong in the past, or is starting to go wrong at present. In a true-life scenario, it is essential to be able to predict likely problems that may arise or accurately recognise failure symptoms when they occur. To achieve this it is important to be able to identify what is really going on and when these facts have been established, to be able to select a suitable means of handling the situation".

Darren Dalcher has been leading Software Forensics research. In [13] he proposed methods for understanding information systems failures. However, examples of disastrous failures abound, some of the most spectacular of which include: Arianne 5 (space disaster); the London Ambulance Service; and most recently, the Tokyo Stock Exchange outage in November 2005.

This paper refers to such failures with a view to highlighting the importance of 'responsibility' and accountability in such systems. The paper then takes a more detailed look at the concept of 'responsibility' within a legal context. Finally we discuss whether IS professionals can be regulated in a similar way to the regulation of professionals in established professions such as medicine and law.

# 2.0 Infamous Systems Failures

## 2.1 Arianne 5

The Arianne 5 space rocket (European Space Agency) ended in failure only 37 seconds from launch. The guidance and altitude systems failed due to loss of information [14]. This was due to specification and design errors in the software of the Inertial Reference Systems (SRI). There were extensive reviews and tests carried out during the Arianne 5 Development Programme. However, they did not include adequate analysis and testing of the SRI or of the complete flight control system, which could have detected the potential failure. The erroneous assumption there was that as the SRI worked for Arianne 4 it would work for Arianne 5 which had a different technical specification.

The Board produced 14 recommendations. Apart from technical recommendations it is interesting to note that recommendations 12-14 (given below) refer to flaws or failures of the process.

> ***"R12*** *Give the justification documents the same attention as code. Improve the technique for keeping code and its justifications consistent.*
>
> ***R13*** *Set up a team that will prepare the procedure for qualifying software, propose stringent rules for confirming such qualification, and ascertain that specification, verification and testing of software are of a consistently high quality in the Arianne 5 programme. Including external RAMS experts is to be considered.*
>
> ***R14*** *A more transparent organisation of the cooperation among the partners in the Arianne 5 programme must be considered. Close engineering cooperation, with clear cut authority and responsibility, is needed to achieve system coherence, with simple and clear interfaces between partners."* [14].

## 2.2 London Ambulance Disaster

The London Ambulance Service (LAS) is the largest in the world, it serves 6.8-10 million people, and comprises 700 ambulances. The complexity of such a system whether manual or computerised is enormous. In October 1992, a major failure of the London Ambulance System resulted in loss of life (up to 20 people died because of late dispatch and arrival of ambulances). Malfunctions and various other problems had been reported earlier but had not been addressed. In one case

alone *"On 7 Feb 1992, an operator inadvertently switched off a screen, losing four emergency calls. On one occasion, the details of a call were lost; the caller called again half an hour later and was told that the details had been lost (by the computer), and an ambulance was dispatched. The patient later died, although it is not proven that there was any link between the delay and the death."* [15]

The LAS Computer Aided Dispatch (CAD) system failure report was presented at the 8th International Workshop on Software Specification & Design by [16] who concluded that *"....it is evident that at the heart of the failure are breakdowns in specification and design common to many software development projects and that the context in which they occurred is far from atypical."*

[13] comments that *"The prevailing culture and the financial climate played a major role in shaping the events that led to disaster. This case study highlights how circumstances can gang-up and the resulting implications to the health and safety of patients."*.

As can be seen in the major report of the inquiry into the London Ambulance Service [17] major flaws in project management, pressure to deliver on time (the CAD system implemented in 1992 was over ambitious and was developed and implemented against an impossible timetable), decision to implement everything in one go instead of adopting a stepwise approach resulted in deficiencies in testing, no effective back-up in case of failure.

### 2.3 Tokyo Stock Exchange outage

Trading on the Tokyo Stock Exchange was suspended for four and a half hours on November 1st 2005 due to a modification of their computer system to expand its capacity. Although this system appeared to be working satisfactorily, it crashed during the automatic monthly clean-up. The back-up system also failed as it was also using the same software [18]

## 3.0 Responsibility, Professionalism and the law

In the three examples given above, the need for safety was of critical importance because of the high price of failure (e.g. losses related to life, finance and opportunity for exploration and experimentation). Where there is such a high expectation of 'safety', it follows that an entity (a person, group or company) or entities should shoulder the responsibility for making these systems 'safe'. Where failures occur, one would therefore expect that whoever has failed in his/her responsibility should incur some type of punitive sanction. It is perhaps surprising that no single person, group or company were prosecuted and held liable for the failures in the examples discussed. The question of responsibility, therefore, is a relevant one to address, especially in light of the increasing use of IS in every facet of human activity. This increasing use of IS demands high standards of professionalism from those entrusted with designing, implementing, managing and

maintaining such systems. Professionalism implies adequate training and knowledge; competence; accountability; care; an understating of ethics and codes of conduct; and the awareness of various social and legal factors [19]. Society, therefore, has an expectation that IT professionals are competent and are aware of their responsibility and the consequences of failure.

The concept of 'responsibility' implies that one is held accountable for his/her conduct in respect of a job, position held or fiduciary duty. While the term 'responsibility' is used in common parlance, perhaps the legal concept of 'liability' more clearly addresses the issue of professional accountability. Liability is defined as 'a legal obligation or duty' [20]. Obligations or duties may arise from contractual agreements and existing laws (statute, common law) among others. Where loss or damage is suffered by a person (organisation or company), liability can be established under various areas of law including: breach of contract; negligence; negligent misstatement; product liability; and professional malpractice [21].

A contract is a legally binding agreement containing various terms (conditions and warranties), that the parties to the contract are obligated to fulfil. Contract terms can be implied into the contract by existing laws (e.g. consumer protection legislation) or expressly stated in the contract document. Contracts are used for the provision of services or products and form the basis on which parties enter into business activities. Where one party to a contract fails to fulfil his/her obligations under the contract then that party is said to be in 'breach of contract', and the other (injured) party is owed a remedy (e.g. financial compensation). The party in breach therefore becomes 'liable' or 'responsible' for not fulfilling his/her contractual obligations.

Negligence relates to torts (i.e. civil wrongs independent of contract). Under certain circumstances a party (e.g. a manufacturer or IT professional) is required to exercise a duty of care to prevent loss or damage to another party (e.g. consumer, end user). Where such a duty of care is owed and is breached (e.g. by careless acts or omissions), leading to consequential loss (i.e. the loss is due to a direct and natural result of the breach of the duty of care) then liability in negligence is established [22]. An injured party can be awarded damages or compensation, and the negligent party can incur financial and/or criminal penalties, depending on the seriousness of the breach.

Tortious liability for negligent advice results in 'negligent misstatement'. Negligent misstatement involves liability for loss due to defective advice given by an expert (person, system) where that advice is intended to be taken seriously and is acted upon. In deciding on liability under negligent misstatement, the expert should have owed a duty of care to the injured party. Such a duty will be imposed by law where there is 'foreseeability' of damage, a proximity in the relationship between the expert and injured party and it is reasonable to impose a duty of care. Where defective advice is obtained from expert systems then the system developer, knowledge expert and other engineers may be liable for negligent misstatement.

A related area of negligence is the concept of product liability, which makes the producer of a defective product liable for any damage resulting from that defect. Further, a consumer can claim against the producer of a defective product regardless of whether a contract exists between the producer and consumer (Consumer Protection Act 1987). While product liability does not apply to software, if defective software is embedded in a product, then this will result in the product itself being defective [22].

Professional malpractice claims address loss or damage caused by negligent or intentional acts committed by a professional in the course of performing his/her duties.

Deciding on who is liable (and therefore responsible) when loss or damage has been suffered usually involves determining who could have prevented the particular loss from occurring. This however, may not be a straightforward case. If full responsibility is placed on one party (say software developers, IT professionals), then, responsibility is removed from the remaining party/parties (e.g. managers or users) [21]. This would involve the latter party/parties not exercising the appropriate level of care needed and hence feeling free to behave in any manner. The law therefore provides a balance (e.g. finding that an injured party may also be negligent) such that all parties need to exercise an appropriate level of care in their behaviour.

# 4.0 Can we learn from other professional bodies?

Generally, professional negligence claims and malpractice lawsuits have been taken against professionals in established professions such as medicine and law. These established professions are regulated by statutory organisations (e.g. General Medical Council (GMC), The Law Society) having: compulsory registration; rules governing conduct and practice; and the legal power to regulate their members.

The GMC [23] was established by the Medical Act 1983 (as amended) [24] and its primary functions are "to protect, promote and maintain the health and safety of the public" (Section 1, Medical Act 1983). All doctors practising medicine in the UK must be registered with the GMC. Under Section 3 ( Medical Act 1983), the GMC had the authority to suspend or remove from the register any fully registered person found guilty of professional misconduct or convicted of a criminal offence. The Law Society [25] regulates solicitors in England and Wales. Its regulatory powers are gained from statute: the Solicitors Act 1974, the Courts and Legal Services Act 1990 and the Access to Justice Act 1999. It has various functions including setting rules of professional conduct, dealing with complaints about solicitors, and disciplining solicitors.

In contrast to doctors and solicitors, IS professionals (programmers, database administrators, systems analysts) are not governed by a regulatory body. Organisations like the British Computer Society (BCS) exist. However, the BCS

for example is simply a registered charity *"to promote the study and practice of computing and to advance knowledge of and education in IT for the benefit of the public"* [26]. The BCS issues codes of conduct and good practice for IS professionals, but there is no obligation on membership and it has no legal authority to regulate IS professionals.

Perhaps the nearest parallells to IS development can be drawn from construction projects such as the design and building of a bridge which involves a large number of people with diverse expertise and with several decision making responsibilities.

The design and construction of IS (especially of large ones) involves designers, analysts, programmers, testers and of course users. In addition, managers, sponsors and strategists play an important role in influencing development, implementation and use issues At each phase of the development decisions of "go/nogo" are taken, deliverables are produced and the next phase is embarked upon. For example, often errors in design are revealed late in the lifecycle resulting in abandonment or rework of the system. Corrective maintenance accounts for 80% of the effort, yet preventative methods have proved to be more beneficial in society (e.g. preventative medicine). Process improvement has long been recognised as desirable for ensuring product improvement. One way of improving the process has been the use of methodologies as a management mechanism, yet systems continue to fail.

A major question then is whether there is the need for a regulatory body for IS professionals. Arguably, a strong regulatory body for IS professionals may help foster a stronger climate of 'responsibility' and accountability in the workplace as seen in other professions like medicine and law. The IS profession however, presents peculiar complexities which may make regulation difficult. To take the analogy of bridge design and construction, if the bridge fails in some way (e.g. the London Millennium Bridge) is it possible to locate the error(s) and more importantly to allocate the responsibility for the rectification/correction of the error(s)? Deliverables of one phase of the lifecycle mould the next phase and determine the quality of subsequent deliverables. This complexity is even greater in IS projects where a fault may lie in any stage of the system lifecycle, e.g. specification, design, software development, implementation phase or otherwise. Further, failure may not only be due to error on the part of an IS worker, but may be in part due to management decisions, user misuse or a "comedy of errors". This leads to the concept of 'secondary liability' (contributory or vicarious) in law. Contributory liability obtains where the injured party has contributed to his/her injury (e.g. a user misusing a system resulting in injury) and vicarious liability obtains where a superior (e.g. manager) is held responsible for the actions of a subordinate (programmer). In deciding who is responsible when failure occurs, liability may not lie at the feet of one particular person but may be distributed among a host of actors in the systems development lifecycle. It is perhaps not surprising then that the accident reports of the various disasters have not resulted in laying blame at any one particular person or category of persons.

The question regarding whether we can learn from other professions must be answered within the context of the complexities of IS system development as discussed above. While the case for regulation is certainly made, the method and mechanisms for implementing such regulation although not obvious may be modelled on existing regulatory bodies. Regulation may need to start at the point of education, setting compulsory standards for qualification and practical training as in the case of medicine and law. In addition compulsory membership of a regulatory body (such as the GMC or Law Society) that has the power to discipline IS workers will have to be enforced.

# 5.0 Conclusions and further research

The issue of responsibility is a serious concern, especially since IS professionals play an increasingly important role in our daily lives. Past failures of safety critical systems, do little to inspire much hope of 'safety' in the future. One good way to promote safety in the future is to ensure that IS professionals take their 'responsibility' seriously and are aware of the consequences of the failure to do so. A regulatory framework might also come to the aid of IS professionals in case of wrongful or malicious accusations that might be levelled against them from persons or organisations. Such a framework will not only engender ethical, moral and legal behaviour by IS professionals but also by the public at large. As discussed previously a major obstacle to devising a regulatory framework for accountability is the complexity of IS projects. We have however, suggested modelling a regulatory framework on existing models such as in medicine and law. A major difficulty may be determining what categories of work need to be made legally exclusive to IS professionals (such as in the case of medical practice or legal practice). This would require legislation to criminalise anyone performing such tasks (e.g. programming, systems analysis and design) without the necessary licence to practice. Such a major shift in employment policy may be justified in the future as we become more and more dependent on IT/IS systems, and the critical roles of IT/IS professionals become inextricably linked to public 'safety'.

# 6.0 References

1 Lyytinen, K. and R. Hirschheim (1987), Information Systems Failures- A survey and classification of the empirical literature. Oxford Surveys in Information Technology. P. I. Zorkoczy, Oxford University Press. 4: 257-309.

2 Moussa, A. and R. Schware (1992), "Informatics in Africa: Lessons from World Bank Experience." World Development 20(12): 1737-1752.

3 Glass, R. (1998), Software Runaways. Upper Saddle River, NJ, Prentice-Hall, Inc.

4 Heeks, R. (2001), "Information Systems and Developing Countries: Failure, Success and Local Improvisations." The Information Society 18: 101-112.

5 Dalcher, D. and A. Genus (2003), "Avoiding IS/IT Implementation Failure." Technology Analysis and Strategic Management 15(4): 403-407.

6 The Chaos Report (1995), The Standish Group http://spinroot.com/spin/Doc/course/Standish_Survey.htm

7 OASIG, The performance of information technology and the role of human and organizational factors, University of Sheffield, 1996.

8 Whittaker, B. (1999), "What Went Wrong? Unsuccessful Information Technology Projects." Information Management and Computer Security 7(1): 23-29.

9 Heeks, R. (2002), "Failure, Success and Improvisation of Information Systems Projects in Developing Countries." The Information Society.

10 Siakas Kerstin V., Berki Eleni, Georgiadou Elli, Sadler Chris (1997): "The Complete Alphabet of Quality Software Systems: Conflicts and Compromises", 7th World Congress on Total Quality & Qualex 97, New Delhi, India, 17-19 February

11 Georgiadou, E. (2003), " GEQUAMO– A Generic, Multilayered, Customisable, Software Quality Model" to appear in *Software Quality Management Journal, Dec 2003*

12 Donaldson A.J.M. & Jenkins, J.O. Systems Failures: An approach to building coping strategy, IEEE Conference on Software Engineering Education & Training, February 2001, Charlotte, NC, USA

13 Dalcher, D (1999), "Disaster in London: The LAS Case study," ecbs, p. 41, IEEE Conference and Workshop on Engineering of Computer-Based Systems.

14 Lions, J. L (1996), ARIANE 5, Flight 501 Failure, Report by the Inquiry Board http://www.cs.unibo.it/~laneve/papers/ariane5rep.html

15 Neumann, P (1992), London Ambulance service computer system problems. The Risk Digest, Vol 12, Issues 38, 1992. http://128.240.150.127/Risks/13.38.html#subj3

16 Finkelstein, A. & Dowell, J. (1996) "A Comedy of Errors: the London Ambulance Service case study", 8th International Workshop on Software Specification & Design IWSSD-8 , IEEE CS Press, 2-4

17 Finkelstein, A. (1993), Report of the Inquiry into the London Ambulance Service. February 1993. http://www.hi.is/pub/cs/2003-04/reliability/topics/LAS/

18 Jaques, R.(2005). Software bug crashes Japan stock exchange. http://www.computing.co.uk/vnunet/news/2145336/software-bug-crashes-japanese

19 Hannabus, S (2000), The issue of professional liability. New Library World, Vol 101, Number 1155, 2000, 97-103.

---

20 Curzon, L, B (1995), Dictionary of Law, 4th Edition, Pitman Publishing.

21 Cardinali, R (1998), If the system fails, who is liable? Logistics Information Management, Vol 11, Number 4, 1998, 257-261.

22 Bainbridge, D (2004). Introduction to Computer Law. Longman: UK

23 General Medical Council: http://www.gmc-uk.org/

24 The Medical Act 1983: http://www.gmc-uk.org/about/default.htm

25 The Law Society: http://www.lawsociety.org.uk/aboutlawsociety.law

26 British Computer Society: http://www.bcs.org/