IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4417

Information Security: A Technical or Human Domain?

Paul Drake and Steve Clarke
The University of Luton, Department of Finance, Systems and Operations
Park Square,Luton, LU1 3JU, Tel: 01582 34111, Fax: 01582 743143, Email: Steve.Clarke@Luton.ac.uk

INTRODUCTION

The ultimate objective of the research study on which this paper is based, is to develop, pilot, and refine an implementation framework for information security, based on critically normative theory. This framework will then be used to critically evaluate existing information security provisions in organisations, including evaluation against existing standards, using case-based and live organisational settings.

The initial part of this study is now complete, and has provided the grounding for achieving the above objectives. This first stage, which is reported within this paper, had the key aim of critically assessing the current status of information security theory and practice from the literature and from empirical evidence. From this, the theoretical constructs that are applicable to an understanding of information security have been determined and are reported. This has led to the consideration of critical theory as a foundation for the domain of information security. An information security framework, based on this work, has been constructed.

Over the past ten years there has been increasing interest in the subject of information security (for example: DoD, 1987; Baskerville, 1988; EC, 1991; O'Connor, 1994; Drake, 1998; BSI, 1999a; BSI, 1999b), with particular emphasis on information technology or computer security (for example: Donovan, 1994; Forester, 1994; Langford, 1995; Neumann, 1995; Gollman, 1999). In the early to mid 1990s, a group of representatives from some of the largest organisations in the UK decided to collaborate to formalise matters. They established a committee under the stewardship of the United Kingdom Department of Trade and Industry and the British Standards Institute to create a British Standard (BSI, 1999a; BSI, 1999b). Each of these organisations (and others) had been working to establish frameworks to adequately secure the information systems within their organisations, and the British Standard had the simple aim of standardising these frameworks into a model that could be applied to any organisation.

There is little doubt that fewer organisations than was expected have embraced the standard. Typically, the most eager to do so have been those originally involved in developing and maintaining the standard (including major multi-nationals such as Shell Oil and Unilever, as well as public sector organisations like Cambridgeshire County Council in the U.K.); and those that have been the subject of adverse external audit reports due to potentially inaccurate information systems or information security incidents such as sabotage and malpractice. Although reliable and auditable information on this latter category is generally not in the public domain, there is considerable evidence to suggest that the trend in the frequency of such incidents is upwards (see, for example: Hosseini, 1990; Stanley, 1994; Young, 1997; Audit Commission, 1998; NCC, 1998; Symonds, 1999).

In this paper it is argued that the reasons why information security has not been widely accepted are not to do with the quality of the standard and how it is maintained, rather, that the current approach to 'information security' is in itself flawed as a concept, and has much to learn from the general domain of social theory.

This study sets out to explore this issue, beginning in the following section, where the current theory and practice of information security is briefly outlined, and is seen to depend on rule-based, technology focussed approaches. The next section critiques this view, and seeks an alternative through a theoretical perspective which, it is argued, better fits the domain. This new approach, based on critical theory, is then discussed as a basis for information security. Finally, a set of principles for applying this latter approach is outlined.

INFORMATION SECURITY: THEORY AND PRACTICE

There is, then, a well established practical basis for information security, but one which has not been adopted as widely as might have been expected. The aim of this paper is to look for reasons why this might be so, and possible alternative approaches which might serve the domain more satisfactorily. Investigations to date suggest poor theoretical grounding for information security as a discipline, with that literature which is available being predominantly descriptive in nature.

An early and still considered seminal work on information security is the United States Department of Defense Computer System Evaluation Criteria (the so called 'Orange Book': DoD, 1987). Although constructed around the security of computer systems to be procured for the US Department of Defense, the document established many of the basic information security principles practised today, and was followed by the European Information Technology Security Evaluation Criteria (EC, 1991). It is in this latter document that the ubiquitous Confidentiality, Integrity and Availability (CIA) principles of information security were first widely documented. CIA embraces the main principles of information security as practised by the industry, the implication of which is that there exists a primary need to restrict information to those entitled to have it, keep it accurate and up to date, and make sure authorised users have access when they need it.

The beginnings of a less rule-based approach to information security are to be found in Russell (1991), who makes an early mention of CIA, but, recognising the common perception that security equates to secrecy (confidentiality), goes on to raise the possibility that integrity and availability may be more important in some environments. This provides the basis for the direction taken within this study, one of the tenets of which is to emphasise the importance of sharing information rather than restricting access to it. To some extent, the aims of confidentiality and of availability may be seen to pull against each other: the more confidential a set of information, the less available it will be. This has raised the

This paper appears in *Managing Information Technology in a Global Economy*, the proceedings of the Information Resources Management Association International Conference.

question of 'available to whom?', and has led to a consideration of information as a human issue, rather than one which is technological or computer-based.

This paper pursues the human-centred theme, and looks for a way forward for information security informed by social theory. There has been considerable discussion concerning the value of social systems theory to information systems in general (see, in the first instance, Hirschheim and Klein, 1989; Hirschheim, Klein *et al.*, 1991; Clarke and Lehaney, 1999a,b), and the section below draws on that background.

INFORMATION SECURITY AS CRITICALLY NORMATIVE SYSTEMS

From the foregoing, it may be proposed that the dominant approach to information security has been pragmatic, based on a rule-based, step-by-step method, rooted in scientific thinking (reductionist, step-wise, and seeking a 'solution' to the 'problem'). From this background, the research study from which this paper is drawn began its search for a basis on which to ground information security. Our proposal is that such a grounding is to be seen as beginning with the Enlightenment, which can be traced to sixteenth century Western Europe. During this time (which embraces the so-called Industrial Revolution centred on the United Kingdom) scientific advancement caused 'instrumental reason', through scientific method, to be privileged ahead of the then dominant religious dogmas.

The outcome of this in terms of how it affects current thinking is that scientific instrumentalism gained precedence, during the 17th Century and beyond, not only over existing religious dogmas, but over *all forms of reason*. Kant (1787) argued that essentially this could be interpreted as 'man' having forgotten how to think unless given rules by which to do so. Kant distinguished between instrumental and practical reason: scientific method, at its extreme, applies only instrumental logic toward truth claims, with the purpose of uncovering objective truths. Kant advocated an "escape from self-imposed tutellage": we had, contended Kant, become trapped in a position where we could think only instrumentally, within laws or rules laid down for us - dialectic or practical thinking was being ignored.

Kantian thought has provided the basis for much of social theory, in particular critical social theory. The idea is that, in a dialectic, reason becomes redefined: it is no longer represented by a vertical process of thought, leading instrumentally to the confirmation or denial of objective truths, but reason is rather concerned with *normative validity*. Whilst the pseudo-scientific process of vertical thinking might be characterised as linear and unreflective, normative validity may be pursued through "dialectical reasoning [which] breaks through the given premises, and frees us to overcome our fixed patterns of thinking – and our being contented with them" (Ulrich, 1983 p.220). From this can be traced Kant's view that *practical* meant that which is possible through freedom, leading to the basic epistemological questions seen to be of value within this study:

What ought we to do	governed by the principle; "design for improvement of the human condition, and reflect on the inevitable *lack* of moral perfection in your designs, *as if* those affected by your designs were self responsible moral beings" (Ulrich, 1983 p.261).

The aim of this will be primarily to challenge what may be seen as the 'illusion of objectivity'. This can be expressed as the belief in truth or facts that are actually not as they seem, but are simply alternative human viewpoints. The aim is a dialectically reasoned position, where reason is defined in terms of normative validity (that which participants, in discussion, agree *ought* to be so).

What may we hope	To be sought through broad involvement of the involved and affected, consultation, and consensus building.

For this we are using participative approaches to explicitly challenge coercion, so that participants (the involved and affected) may meaningfully participate.

All of this points strongly to the critical stream of thinking being of value as an alternative view in a predominantly rule-based domain such as information security. This critical stream has been taken forward, since the 1920s, by first the Frankfurt School, and latterly Foucault and Habermas (for an outline, see Brocklesby and Cummings, 1996). In the UK, it has been used as a basis by critical systems thinkers within the systems movement (see, for example, Jackson, 1985; Flood and Jackson, 1991; Jackson, 1991; Mingers, 1997).

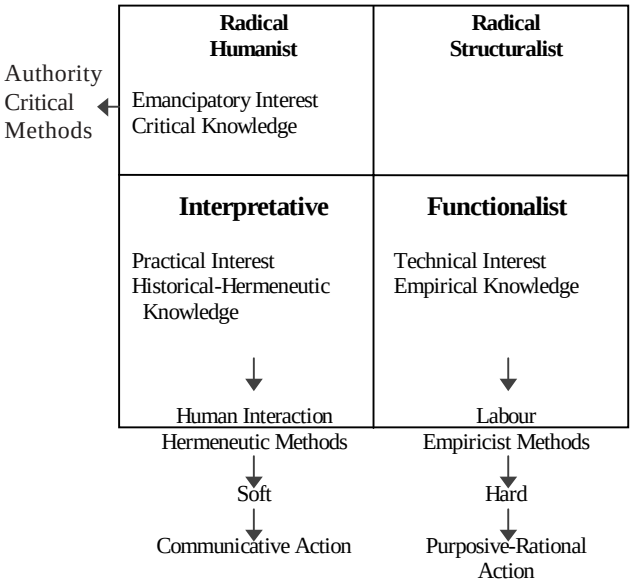
Information security, then, may be seen as having been approached to date as a pseudo-scientific domain, but one which lacks a convincing, and explicitly articulated, theoretical base. The tenets of scientific method are to be found in its reliance on an instrumental approach, but this appears as an impoverished view of the domain, privileging confidentiality rather than openness and information sharing. This study, by drawing on theoretical and practical work within critical systems theory, seeks to develop an alternative theoretical, and hence practical, framework for information security.

CRITICAL THEORY AS A BASIS FOR INFORMATION SECURITY

The relevance of the domain of critical theory to information *systems* has been explored extensively (Lyytinen and Klein, 1985; Klein and Hirschheim, 1987; Hirschheim and Klein, 1989; Gregory, 1993; Kirby, 1993; Fitzgerald, 1996; Clarke, 1997; Clarke and Lehaney, 1997; Lehaney and Clarke, 1997; Clarke, 2000). This paper seeks to pursue the critical strand and relate it more directly to the study of information *security*. Much of the available literature focuses in principle on the philosophy of science (in which it is argued that the search for 'truth' is grounded in positivism), and the philosophy of social science (wherein the search for 'truth and reality' are pursued from an anti-positivistic position, and techniques such as advocacy, persuasion and coercion, dominate). These arguments may be represented as predominantly paradigmatic, relying on the paradigm incommensurability thesis, for which the four paradigms of Burrell and Morgan (1979) is still a pre-eminent representation. Figure 1 summarises this position through an expansion of the Burrell and Morgan grid (Clarke, 2000: after Oliga, 1991).

Burrell and Morgan argue that all social theories can be categorised within this framework. Business organisations, it is held, concentrate mostly on functionalist approaches, following an instrumental rationality based on the methods of the natural sciences. This is the position outlined as fundamental to information security in the early part of this paper: based on 'hard facts' and focusing on technological issues. Whilst interpretivism was seen, at an early stage of this research, to be a valuable potential direction, the freedom to contribute or participate, which lies at the heart of radical humanist approaches, increasingly emerged as a

Figure 1 The Social Validity of Hard, Soft and Critical Approaches



key requirement to support the strength of the hermeneutic method. Put simply, without free and open participation, interpretative approaches are destined to fail; but such open participation, whilst a ***requirement*** of interpretative method, is not ***ensured*** by it.

In this way, Figure 1 can be used to show how Burrell and Morgan's typology might be interpreted within information security. The proposed move to critical theory essentially seeks paradigmatically to push information security from bottom right to top left, and to help in achieving the 'critically normative' approach to information security which this research has identified to be of value to the domain.

Information security, then, is grounded in the philosophy of science: it is substantially rule-based and instrumental: BS7799, the British Standard, is intended to be auditable, and must be specific; the process of certification is based around compliance or non-compliance. But we are nevertheless left questioning the very standards themselves, and looking for an improved way forward.

TOWARD A 'CRITICALLY NORMATIVE' MODEL OF INFORMATION SECURITY

This approach draws on Ulrich (1983; 1991), applying critique in three ways: firstly to surface the normative content of systems designs; secondly it is applied to boundary judgements in helping determine the system of concern; and thirdly critique is undertaken to reveal the normative content in 'system' – to challenge "objectivist delusion".

> "The key problem that makes applied science, as compared with basic science, so difficult to justify lies in the *normative content* that its propositions gain in the context of application" (Ulrich, 1991).

The important distinction made is between theoretical reason, applied instrumentality to determine truth claims, and practical reason, concerned with the normative validity of practical propositions: reason is " .. theoretical if it secures critical understanding of *what is*; (and) practical if it secures critical understanding of *what ought to be* (Ulrich, 1983 p.220).

From this perspective, information security no longer takes the position of instrumental decision making according to a certain set of norms, but may be seen as 'rational' if those involved in and affected by the system of concern "make transparent to themselves and to each other the normative content" (after Ulrich, 1983). The critical thrust of this approach requires that the interventionist apply critique not merely against a set of norms, but against the norms themselves, making the critique self-reflective or 'practical' in Kantian terminology. It involves surfacing the values or norms that underlie the position taken or judgements made. A dialectical approach is seen to be essential here, the purpose of the dialectic (Ulrich, 1983 p.289) being to bring together all participants in the process through a discourse which surfaces their normative positions.

To intervene within a problem context requires that the scope of that context be defined. In systems terms this requires determining the boundary of the system, but frequently this is done in an arbitrary and uncritical way. Ulrich (1991) advances the view that boundaries are most frequently drawn to include that which is controllable. In response to this he calls for a "critically normative understanding of boundary judgements" (Ulrich, 1983 p.25).

A further theme inherent in Ulrich's (1988) work is that of emancipation to combat coercive influences. Here he draws on Habermas (1971, p.240), who asserts that, in both theoretical and practical reason, decisions are reached by "the peculiarly unforced force of the better argument" rather than by resort to power or deception. Ulrich (1983 p.221) also refers to Kant's moral idea, which introduces emancipation to the debate: "By 'the practical', I mean everything that is possible through freedom" (Kant, 1787, p.828).

The critically normative approach to information security (Table 1) presents a very different picture of the future of the domain to the one currently favoured.

Table 1 An Alternative Future for Information Security

The Current View	**The Proposed View**
Confidentiality / Restriction	Availability / De-restriction / Sharing
Information Restriction	Information Sharing
Pragmatic	Theoretical / Empirical
Technological / Computer Systems	Human Activity Systems
Instrumental	'Practical' Critically Normative. Apply Critique to: Normative Content Norms Boundary Judgements 'System'
Pseudo-Scientific	Social
Rule-Based	Challenge the Rules
Truth	Normative Validity
Formal-Logical: Unreflective	Dialectical: Free to Think
'Is'	'Ought'
Functional	Radical
Accept the 'Material Conditions'	Critique of 'Material Conditions'
Rational equals Seeking the 'Truth'	Rational equals a dialectic between the 'involved and affected', all of whom are free to contribute

The 'current view' may be seen as a set of guidelines or principles on which present approaches to information security are explicitly or implicitly based. The 'proposed view' provides the foundation for moving ahead now to achieve the ultimate objective of this study: "to develop, pilot, and refine, an implementation framework for information security, based on critically normative theory."

CONCLUSIONS

A Kantian approach, together with the interpretations of it by critical thinkers, has led to our questioning the basis for a theory and practice of information security. Instrumental or theoretical reason, by focusing on producing *objective knowledge*, seems an impoverished view when compared with the insights generated through practical reason. Practical reason, with its critically in-

formed search for that which *ought* to govern our social world, has the potential to free us from the rule-based traps we have fallen into.

It is planned, therefore, that a critically normative approach to information security now be developed, based on relevant social theoretical constructs, and focusing primarily on critical theory. The aim is to build a system of information security based on a critically informed dialectic, where the normative content of the system, its boundaries, and the material conditions within which it is presently perceived, are all open to challenge and open debate. All those involved in and affected by the system of concern should participate, with an emphasis on information sharing rather than restricted access to information, and with the overall objective of determining what the system *ought to be*, not what it *is*.

This proposed journey from instrumental to practical reason as a basis for information security will be a long one, but our research has, we believe, demonstrated it to be worthy of further development. For our part, with the first phase of theoretical analysis substantially complete, we are now concentrating on the design of a framework for information security, and testing that framework in empirical application.

REFERENCES

Baskerville, R. (1988). *Designing Information Systems Security*, Wiley.

Brocklesby, J. and S. Cummings (1996). "Foucault Plays Habermas: An Alternative Philosophical Underpinning for Critical Systems Thinking." *Journal of the Operational Research Society* 47(6): 741-754.

BSI (1999a). Code of Practice for Information Security Management. BS7799 part 1. London, British Standards Institute.

BSI (1999b). Specification for Information Security Management Systems, BS7799 part 2. London, British Standards Institute.

Burrell, G. and G. Morgan (1979). *Sociological Paradigms and Organisational Analysis*. London, Heinemann.

Checkland, P. B. (1989). "Soft Systems Methodology." *Human Systems Management* 8(4): 273-289.

Checkland, P. B. and M. G. Haynes (1994). "Varieties of Systems Thinking: The Case of Soft Systems Methodology." *System Dynamics* 10(2-3): 189-197.

Clarke, S. A. (1997). Critical Complementarism and Information Systems: A Total Systems Approach to Computer-based Information Systems Strategy and Development. *Information Systems and Computing*. Uxbridge, U.K., Brunel: 313 Pages.

Clarke, S. A. (2000). From Socio -Technical to Critical Complementarist: A New Direction for Information Systems Development. *The New SocioTech: Graffiti on the Long Wall*. E. Coakes, R. Lloyd-Jones and D. Willis, Springer, London, 61-72.

Clarke, S. A. and B. Lehaney (1997). *Critical Approaches to Information Systems Development: A Theoretical Perspective*. Systems for Sustainability: People, Organizations, and Environments, Milton Keynes, U.K., Plenum: 555-560.

Clarke, S. A. and B. Lehaney (1999). "Human Centered Research and Practice in Information Systems." *Journal of End User Computing* 11(4): 3-4.

Clarke, S. A. and B. Lehaney (1999). *Human-Centred Methods in Information Systems Development: Is There a Better Way Forward?* Managing Information Technology Resources in Organisations in the Next Millennium, Hershey, PA, U.S.A., Idea Group Publishing: 585-592.

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

DoD (1987). US Department of Defense Trusted Computer System Evaluation Criteria (The Orange Book). Washington DC, US Department of Defence.

Donovan, S. (1994). *Approaches to Access Control*. European Security Forum, Koln, European Security Forum.

Drake, P. (1998). The Use of Information Security Theory in Practice. *Anglia Business School*. Cambridge, Anglia Polytechnic University: 77 pages.

EC (1991). Commission of the European Communities, European Information Technology Security Evaluation Criteria (ITSEC), European Commission.

Fitzgerald, B. (1996). "Formalised Systems Development Methodologies: a Critical Perspective." *Information Systems Journal* 6: 3-23.

Flood, R. L. and M. C. Jackson, Eds. (1991). *Critical Systems Thinking: Directed Readings*. Chichester, Wiley.

Forester, T. M., P (1994). *Computer Ethics*, Massachusetts Institute of Technology.

Gollman, D. (1999). *Computer Security*, Wiley.

Gregory, F. H. (1993). "Soft Systems Methodology to Information Systems: a Wittgensteinian Approach." *Journal of Information Systems* 3: 149-168.

Habermas, J. (1971). *Theory and Practice*. Boston, Mass, Beacon Press.

Hirschheim, R. and H. K. Klein (1989). "Four Paradigms of Information Systems Development." *Communications of the ACM* 32(10): 1199-1216.

Hirschheim, R., H. K. Klein, et al. (1991). "Information Systems Development as Social Action: Theoretical Perspective and Practice." *Omega* 19(6): 587-608.

Hosseini, J. C. A., R. L. (1990). "Randomised responses a batter way to obtain sensitive information." *Business Horizons* Vol. 33, no. 3: 82 - 86.

Jackson, M. C. (1985). "Social Systems Theory and Practice: The Need for a Critical Approach." *International Journal of General Systems* 10: 135-151.

Jackson, M. C. (1991). *Five Commitments of Critical Systems Thinking*. Systems Thinking in Europe (Conference Proceedings), Huddersfield, Plenum: 61-72.

Kant, I. (1787). *Critique of Pure Reason*. London (1929), Macmillan.

Kirby, M. A. R. (1993). *Improving the impact of Systems Thinking on Information Systems Development*. Systems Science: Addressing Global Issues (Conference Proceedings), Paisley, Plenum.

Klein, H. K. and R. Hirschheim (1987). Social Change and the Future of Information Systems Development. *Critical Issues in Information Systems Research*. R. J. Boland and R. A. Hirschheim. Chichester, Wiley: 275-305.

Langford, D. (1995). *Practical Computer Ethics*, McGraw-Hill.

Lehaney, B. and S. A. Clarke (1997). *Critical Approaches to Information Systems Development: Some Practical Implications*. Systems for Sustainability: People, Organizations, and Environments, Milton Keynes, U.K., Plenum: 333-338.

Lyytinen, K. J. and H. K. Klein (1985). The Critical Theory of Jurgen Habermas as a basis for a Theory of Information Systems. *Research Methods in Information Systems*. E. Mumford, R. Hirschheim, G. Fitzgerald and A. T. Wood-Harper. Amsterdam, Elsevier: 219-236.

Mingers, J. (1997). Towards Critical Pluralism. *Multimethodology: Towards Theory and Practice of Integrating Methodologies*. J. Mingers and A. Gill. Chichester, Wiley.

NCC (1998). NCC IT Security Breaches Survey. London, Na-

tional Computer Centre & Department of Trade & Industry.
Neumann, P. (1995). *Computer-Related Risks*, Addison-Wesley.
O'Connor, G. C., M (1994). *Raising Awareness*. European Security Forum, Koln, European Security Forum.
Oliga, J. C. (1991). Methodological Foundations of Systems Methodologies. *Critical Systems Thinking: Directed Readings*. R. L. Flood and M. C. Jackson. Chichester, Wiley: 159-184.
Russell, D. G., G (1991). *Computer Security Basics*, O'Reilley & Associates Inc Stanley, A., Edwards, R & Aherne, J (1994). *The 1994 Security Status Survey*. European Security Forum, Koln, European Security Forum.
Symonds, M. (1999). "A survey of business and The Internet." *The Economist*(Q1): 240.
Ulrich, W. (1983). *Critical Heuristics of Social Planning: A New Approach to Practical Philosophy.* Berne, Haupt.
Ulrich, W. (1988). "Systems Thinking, Systems Practice, and Practical Philosophy: A Program of Research." *Systems Practice* 1(2): 137-163.
Ulrich, W. (1991). Critical Heuristics of Social Systems Design. *Critical Systems Thinking: Directed Readings*. R. L. Flood and M. C. Jackson. Chichester, Wiley: 103-115.
Young, E. (1997). Global Information Security Survey. London, Ernst & Young International.