35

Developing Policies, Procedures and Information Security Systems

Dr. Adrian R. Warman,
Department of Management Systems, Bournemouth University,
Bournemouth, Dorset, BH12 5BB, United Kingdom
email: awarman@bmth.ac.uk

1. INTRODUCTION

This paper reports on findings from current research into the development of Information Security Policies within Organisations. The work highlights the key issues that influence the development of policies, procedures and information systems, in the context of information security provision. Going further, it identifies aspects of current practice in Information Security Policy Development that challenge the success and long-term viability of organisational processes for identifying, designing and implementing appropriate and sufficient protection measures. This information is then used to make recommendations for organisations attempting to develop their own effective policies.

2. INFORMATION SECURITY

For most organisations, the provision of information security requires consideration of a broad range of activities, including but not limited to the prevention of theft, blackmail, and fraud; all various manifestations of Computer Related Crime (CRC). It is not our intention here to define in detail what is meant by CRC. Good discussions that expound upon various interpretations and definitions of CRC can be found in [1], [2], [3], and many other sources. We are however interested in looking at how CRC is dealt with by organisations through the use of information security strategies and mechanisms.

In 1991, the author initiated work in this area, focussing in particular upon policy development, producing results reported in [4] and analysed in [5]. An important question is whether organisations have made progress since then in understanding the issues surrounding computer security, both in terms of the technological factors that provide threat and defence mechanisms; and with regard to the development of appropriate defensive infrastructures. It is suggested that perception of information security is significant for modern organisations, because it directly influences awareness of, and reaction to, the threats to data processing and information-providing resources. Crucially, there

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

is a difference in the way in which we understand and interpret security issues, according to whether we focus on the individual, or the organisational perception of what security objectives are sought.

2.1. Individual and organisational perceptions

Generally, the two perceptions are well understood and documented. For the individual, a breach of security may be experienced as a loss of data, or loss of access to resources. A security failure of this kind will tend to result in two types of outcome for the individual. The first is inconvenience through time lost to recover the data or re-enable access. The second is from the implications of having data or access available - even if for a short time only - beyond the domain of authorised users. The problem is that losses of this kind may also be confused with simple systemic inadequacies or failure, yet must be addressed in a different fashion.

For the organisation, provision of information security can have a much more profound effect, in terms of demands on time, money, or other corporate resources. Yet any occurrence of CRC provides damning evidence of the inadequacies of the implemented security or operational techniques, which can severely undermine the credibility of the organisation. Lack of attention to information security may also provide strong evidence of a weak or misdirected organisational culture. Sensitivity to security matters is either not appreciated or not applied, an organisational characteristic of neglect that may derive from the highest board room levels [4].

2.2. The implications of perceptual differences

This contrast in perception of security may have its origins in the different perceptions of the information systems themselves. Organisations typically view information technology as 'a good thing'. This is because when applied constructively and efficiently, IT increases productivity and data availability, while reducing the costs of employing large numbers of staff. However, the parallel short-term view taken of initial system provision, such as installation, training and operating costs, may often be considered 'a bad thing' by those who must evaluate the expenditure against other organisational demands. Such a view may also be extremely dangerous if not thought through carefully, as evidenced by the often advertised and increasing demand for temporary or contractual staff with computing skills. The trend continues to suggest an emphasis on computing skills in particular, when a more realistic requirement is likely to be for the individual to have an understanding of *corporate* information needs, and the corresponding use of computer and other information technology systems to *support* these needs.

Accordingly, data and information processing resource provision will inevitably be perceived in various ways. Such differences can lead to potentially incompatible individual and organisational agendas. In other words, the significance of the contrast in perception is that it affects the way in which information security is dealt with at end-user and organisational levels. As a consequence, the mechanisms for providing a defence for such systems must be developed, installed, operated and administered in a fashion that takes account of different viewpoints. In this sense, information security is perhaps like any other issue that faces the organisation. A matter needs to be dealt with, there are a number of positions to be considered, a set of possible responses is identified, and one is chosen and implemented. The problem is that the issue of information security is *not* just like any other problem within an organisation.

As a natural result of the way that most organisations work, many of the mechanisms for dealing with most matters in the organisation are constructed from policies and procedures. It is therefore natural for specialists, a term which in this context includes business-ignorant technologists just as much as technophobic managers, to apply similar approaches and techniques according to their perception of security problems, because of the familiarity of the working domain.

Another important characteristic of policies and procedures is that they are often used to identify responsibility, or for the individual to hide behind. In other words, policies and procedures are also used to enable the individual to be sure that since they have acted in accordance with stated procedures, they cannot be blamed for any inadequacy of the outcome.

Problems such as these mean that the process of addressing security by the development of policies and procedures derived through *conventional* business processes alone must now be challenged, because of the special circumstances dictated by information resource defence requirements. In order to understand why, we must first speculate over the way in which attacks on information systems are likely to evolve in the future.

3. WHERE IS CRC GOING?

If there is already some room for debate over what precisely CRC is, then the nature of CRC and related problems for information systems in the future is even more subject to disagreement. For example, the boundary between genuine CRC, and system failure or even mal-implementation is likely to become increasingly subject to confusion and possibly deliberate blurring. Too often, 'computer error' is used as an excuse for personnel errors, which are themselves often the result of either implementation or operational mistakes.

However, it is possible to identify some of the current catalysts that are affecting information systems in general, and security in particular. An important example is observed by considering the trends in the installed base of home computers, and particularly computers in schools (figure 1), both of which show inexorable increases each year.

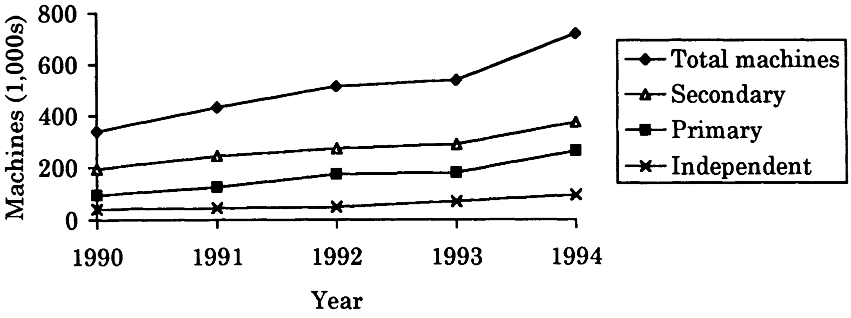

Figure 1: Computers in schools (UK market figures for one supplier)
Source: Acorn Computers Ltd., 1994

These trends illustrate the widespread and increasing acceptance of computer technology in all aspects of everyday life. People of all ages are now used to interacting with computer systems in a directed rather than ad hoc manner. This means that society can no longer depend on ignorance or fear of the technology as mechanisms to control the way in which technology is used. Another example comes from the increasing popularity of dedicated games consoles. While it is easy for professionals to disdain such systems in terms of contribution to technical or systemic concepts, there can be little doubt that they influence the perception of technology today. In conjunction with advances in Human-Computer Interaction techniques, entertainment systems have an effect in encouraging users, and particularly the up-and-coming generation of soon-to-be end-users, to exercise technology to its limits. The importance of 'fun' in learning has long been recognised, not least by developers, who respond in a number of ways, for example describing their work as being the provision of 'edutainment'.

Some home entertainment magazines provide information about special 'cheat' modes for games, often used by developers to test the games during construction, but subsequently sought out and paraded almost as trophies by end-users. These are often found by repetitively trying out unusual key sequences. The danger is that the same enthusiasm for using different techniques to locate the short-cuts in games may also be akin to the motivation and methods used by security penetrators. Given this possibility, entertainment systems may support the development of a mentality and even a form of 'training ground' for computer attacks.

These observations, coupled with the inevitable conflict between the interpretation and implementation of organisational and personal agendas, mean that the threats against organisational information systems are now, and will continue to be, an inherent and increasingly unpredictable inevitability. The rapidly increasing capabilities of information systems, which it seems are not being matched by corresponding advances in the theory or application of social or managerial disciplines, put such threats on a path of inevitable growth that will become ever more unstructured, uncertain, and dangerous. Aggregating the capabilities of technology today, such as global internetworking and virtual reality systems, with the concerns over the variety and incompatibilities of national and international computer related legislation, and we uncover disturbing inadequacies in conventional organisational approaches to information security.

4. ORGANISATIONAL APPROACHES TO INFORMATION SECURITY

In trying to protect information systems, organisations will address three business fundamentals.

The *objectives* of protection are defined in terms of statements that describe how the individual or organisation will ensure a continual move towards the successful attainment of the goal of securing the system.

The *goal* of protection is usually to ensure that no loss occurs to the organisation or the individual as a result of actual or attempted attack on the data resource. The loss may be in terms of access to data or resources, or loss of confidentiality. The goals themselves therefore represent identifiable measures by which the organisation recognises success, a particularly difficult concept with regard to CRC.

Supplementing these will be *aims* that are longer-term concepts, whereby having achieved the goal the organisation wishes to ensure that the loss-prevention is maintained on an on-going basis. Aims are therefore the end result of on-going success in achieving the goals.

The importance of objectives, goals and aims is in helping the organisation and individual to identify their mission and means of achieving the desired results. The outcome of the identification process will be, amongst other things, policies and procedures.

In the context of information security, two major difficulties arise for organisations when we try to apply the concepts of Objectives, Goals and Aims.

The first is that even within the 'pure' business domain, there is frequently a confusion over the three concepts, and this confusion will adversely affect the vision and focus of those trying to work within the situation. Many organisations, and an even larger number of managers, fail to grasp the distinction between the concepts, or have even thought about the implications of the distinction on the way that they work. The result is a weak appreciation of the focus and direction of the mission.

The second difficulty is that a goal should ideally be something that can be clearly measured in tangible terms. Yet with information security, the goal simply cannot be achieved.

As systems are made more secure, and the goal is brought closer, so usability of the system is likely to decrease due to the number of passwords, domain controls, and other security mechanisms. Additionally, the cost of the system is likely to increase as more protection mechanisms are implemented both internally and externally.

4.1. The current situation

In order to support their activities, organisations today have access to a wealth of resources. These include technological tools and information systems for implementation of specific tasks, and administrative and organisational tools used for evaluating the outcome from the information systems and subsequently addressing the larger scale and more unstructured problems of managing and directing the organisation.

A highly simplistic definition of an information system within the context of information security is a collection of technical and administrative resources that are configured and integrated to perform tasks of measurable value to the user or owner organisation.

These administrative tools include two major concepts: policies and procedures.

A helpful definition of policies can be found in [6], which states that a policy is 'a standing plan that establishes general guidelines for decision making'. This definition, along with similar ones in other texts that managers might read to develop their skills, has two important implications. The first is that the content of a policy will be generalised in nature, rather than specific. This has the advantage of flexibility, but the disadvantage of reducing the ability to define a specific response. Of course, it could be argued that specific responses are defined within the context of procedures, but that is a point to which we will return.

The second implication in the definition of policies is that they are used in decision making. In other words, there is an element of latitude in the interpretation of circumstances. This is obviously extremely helpful, and is frequently used by UK Police officers in determining whether to make a formal charge or to issue a caution. Nevertheless, in the context of information security, the freedom implied by a policy may be entirely inappropriate. Reinhardt's description of the Internet in [7] is also indicative of factors relating to attacks on information systems. He notes that the Internet is 'a government-subsidised experiment in distributed computing, electronic community, and controlled chaos. ... If the wires and cables of the communications industry are the data highway's foundation, the Internet may provide its language, culture and customs.'

Stoner also provides a useful definition of procedures, which are 'detailed guidelines for handling organisational actions that occur regularly'. Here, we might expect to have more prescriptive instructions on how individuals or the organisation should provide information security, and indeed the definition does indicate that procedures should provide more detail. Yet the use of the word 'guidelines' undermines the importance of precision. The definition also suggests that procedures tend to relate to repetitive or frequently occurring events. This is in contrast to the desired situation, which is that an organisation will not experience security breakdown or CRC on a frequent basis! As a result, the role of procedures, and indeed the mechanisms by which they are developed, are not necessarily compatible with the provision of information security.

The problems that policies and procedures entail for organisations have led to more than one source suggesting that organisational effort expended on them should be reduced to a minimum. Tom Peters suggests in [8] that we must 'radically reduce and simplify paperwork and unnecessary procedures', and makes the point that 'Quick response to perpetual turmoil is now a competitive necessity' - a highly apposite observation in the context of information security.

5. INFORMATION SYSTEMS AND ORGANISATIONS

At the heart of the problems that organisations face is the fact that they now have increasing access to powerful yet cheap information technology systems and data repositories. These resources are being applied by organisations and end-users through the use of dated and even inappropriate management processes, that may themselves be poorly understood and resistant to qualitative and quantitative evaluation.

Until recently, the benefit of IT for most organisations was predominantly in performing existing tasks more quickly. Yet the ability of IT systems to cross-reference and present data in innumerable forms is still poorly appreciated and even more poorly utilised. Instead of becoming data pools that organisations can benefit from, too many data bases are becoming congested data swamps.

As an example of the speed of development and enhancement to capabilities, Odd de Presno reports in [9] that on Friday, Feb. 26 1993 at 12:18 p.m., a bomb exploded in the World Trade Centre in New York City, USA. Four minutes later, the Dow Jones News Service flashed the headline: 'NYC Fire Dept. Says Fire At World Trade Center.' Few organisations are able to accommodate the implications of such rapid information dissemination, or effectively integrate such a resource into their strategy for competitive advantage.

The status symbol of having a high-performance computer system on the desk of each senior executive, even though the machines are rarely switched on, let alone utilised to great effect, is still a too frequent occurrence within organisations. Use of technology and the surrounding information system is too often perceived as a low-level activity. The result is that 'hands-on' knowledge, and therefore understanding, of the systemic strengths, weaknesses, opportunities and threats that Information Technology represents is absent from board room strategic deliberations. Appreciation of the possibilities of information systems in supporting strategic activities is extremely rare and underdeveloped. Thus, by isolating information systems at a distance from the strategic directional work, many organisations are actually facilitating the failure of security through low-level activities.

There is also the danger that some perpetrators of CRC are implicitly or even explicitly admired for their skill and expertise, as indicated by some reports carried in newspapers or articles, although this trend may be improving as time goes by. The improvement may not be as a result of a maturity of approach from reporters, but rather the reducing interest that such reports produce. This may be explained by the increasing awareness and perhaps cynicism that most people now have regarding computer systems. Events that involved computers and which might once have produced screaming headlines are now much more likely to be relegated to the inner pages of newspapers, even those publications that specialise in computer issues.

5.1. Current practice in information system security policy development

These observations are supported by results from research carried out by the author in Winter 94/95. One hundred UK national organisations that are major users of information systems were surveyed to establish details of their computer security policies. The organisations ranged in size from 30 to over 80,000 employees, covering market sectors such as banking, education, utility services, defence, and software development. Respondent titles included IT Security Manager, IT Manager, Systems Manager, and Office System Development Manager. All respondents had the option to remain anonymous in their replies, although all were encouraged to provide some form of contact details so that follow-up work could be performed.

The determination of security policy is still taking place at a low level within organisations. The results indicate that board level involvement with policy development remains minor. Similarly end users have only limited involvement, although their requirements are seen as being significant factors to take into account. More positively, divisional or departmental managers and team or group managers have a significant role in policy development. The trend indicates that recognition of security issues is indeed moving up the corporate agenda from localised operational consideration to higher levels. However, the progress made over the last four years is slow (the last survey took place in 1991, and is reported in [4]).

The publicity given to threats is clearly a major influence in determining policy development, in contrast to expert consultancy advice which continues to have only a minor role. Indeed, such publicity - whether through case studies or media reports - is generally welcomed as helping to promote awareness of computer security within organisations.

It is interesting therefore to note the contrast between the ideas and theory of security policy that appear to be recognised and accepted, and the actual practice of their implementation within organisations. In an attempt to understand this discrepancy, discussions were held with identified respondents from organisations exhibiting the disparity, providing information that underpins many of the ideas presented in this paper.

6. ASSUMPTIONS THAT ARE NO LONGER VALID IN SECURING INFORMATION SYSTEMS

We have now reviewed three key factors that relate to information security. They are the changing nature of information security itself, the use of policies and procedures to provide appropriate security controls, and the nature of information systems within organisations.

The combined effect of these factors makes it imperative that we challenge existing assumptions and methods of dealing with information security. Evidence indicates that such assumptions are inadequate in supporting effective consideration of the issues.

6.1. Assumption: That the freedom of policies, and the constraints of procedures, are sufficient and appropriate in securing information systems

CRC is frequently a low-level activity, that takes place by influencing or interacting with the micro-level within organisations. For example, a member of staff may subvert or 'enhance' an existing process to acquire additional funding or resources. In everyday terms, this may be illustrated by reference to the 'old boy network', or gaining information or access through the 'grapevine'.

Yet the development of policies and corresponding procedures is often inspired and dictated from the higher macro-levels. Even when freedom of interpretation is intended for policies, or to a lesser extent procedures, directives of this kind ultimately depend upon an essentially inflexible recognition of, and respect for, control within the organisation. However, CRC and Information Security threats often arise by circumventing such control structures.

In order to address this problem, organisations will have to reconsider the arrangements by which information systems integrate into the business processes, as indicated in the second assumption.

6.2. Assumption: That our understanding of the relationships between business and technology is progressing well, and will continue to do so

It is already difficult enough trying to place some form of structure onto the various kinds and implementations of management methods, owing to the variety and incompatibilities between them. It is not easy to identify a widely acceptable 'unified' approach for dealing with management issues.

Our understanding of technology application is in a similar weak state, and the problem is exacerbated by the dynamic and unpredictable nature of the subject. The high speed of development means that state-of-the-art equipment becomes antiquated and obsolete in a time-scale measured in months or even days, which makes on-going understanding of the issues extremely difficult to maintain.

Given the significant differences between the two domains, there is no reason at all why our understanding of the relationship should be making progress in any but the smallest of steps. Indeed, some organisations are perhaps starting to accept that they cannot easily integrate business and technology without fundamentally replacing core structures, even though they will openly acknowledge the importance of doing so. It may be that it is for this mis-guided reason that consideration of technology and information systems is relegated to the lower levels within the organisation.

The interface between these two domains needs to be more clearly defined in order to address information security. More usefully, organisations with a high or increasing dependency upon information systems will have to take account of the fact that meaningful introduction of the system will require a fundamental reconfiguration of traditional business processes. As technology-based systems are integrated into the organisation, so the capabilities of information users and demands on information providers will increase, as will the complexities of the information flows themselves. An *efficient* dynamic information network, that builds and removes channels upon demand, is unlikely to be compatible with formalised organisational structures such as policies and procedures.

6.3. Assumption: That information security is ultimately a people-problem or a technology-problem

When protecting systems, by far the most common approaches suggested are to implement secure mechanisms for the system, or to train or increase the awareness of staff and end-users. Of course, an unknown person using a resource within the organisation should be challenged, but this may be an increasingly common occurrence in the typical business today, given the trend towards temporary or contract staff. If the source or cause of security breakdown is thought to be from the staff alone, then the problem is dealt with by using people-centred approaches. Such approaches are not necessarily wrong in themselves, but are unlikely to be adequate unless supplemented by other methods.

Similarly, if the problem is thought to be from systems that are too open or easy to use, then constraints are built in to them. These include increasing the number of access control levels, which may break down the earlier uniform operational capability into new domains, to which the user may, or may not, have access. Far from improving the situation, this may actually exacerbate it, or even pre-empt aggressive action, because of the additional difficulties and frustrations caused to the authorised end-users.

Using either a people- or techno-centric approach fails to recognise the importance of an integrative foundation for dealing with the issues. It also denies the nature of the increasingly important but still poorly appreciated link between business and technology disciplines.

Again, part of the solution may be found in a reconsideration of the way in which information systems and business structures are to be integrated.

6.4. Assumption: That having a policy means we have the latitude, and know how to deal with the unexpected, which of course we are expecting anyway

Latitude in interpretation of events and how to react to them is extremely important. However, the current approaches for developing policies may simply be inappropriate.

An example of the kind of problems encountered can be found in the US General Accounting Office report on Computer Security in Government Planning Processes [10]. The Computer Security Act of 1987 requires 'federal agencies to identify systems that contain sensitive information and to develop plans to safeguard them'. The summary of the results of the report, which involved approximately 60 civilian agencies, contains some telling issues:

'Officials cited three problems relating to the design and implementation of the planning process: (1) the plans lacked adequate information to serve as management tools and some agencies already had planning processes in place, (2) managers had little time to prepare the plans, and (3) the Office of Management and Budget (OMB) planning guidance was sometimes unclear and misinterpreted by agency officials.' [10]

Thus latitude and flexibility in interpretation may not produce the desired results, even where there is a clear mandate and priority to do so.

7. RECOMMENDATIONS

The changes that will take place in both technology-based information systems and the consequent information security requirements are inevitable. The uncertainty and instability that these will cause will be made worse by the imminent arrival of the new young 'cyber-punk' generation. For them, 'surfing the Internet' is as common a practice as hanging around on street corners. The power of the resources that they can call upon and apply, coupled with the anarchy of approach that they adopt, will drastically reshape organisations and their processes.

In the short term, organisations must stop playing games with the information resources. It is imperative that they work towards a resolution of the issues, and integrate information system issues into prudent as well as best business practice. This matter is too important to be constrained by politics, because it is already too difficult trying to get things to work when there is agreement and co-operation, let alone when there is not.

Conventional perception and determination of 'best practice' in Information Systems Security within the organisation must be challenged. How is it to be determined in the future? How is it measured? Why is it that measures are implemented in the way they are, and are such measures sustainable in the long term? What criteria have been used to evaluate relevance and success in dealing with the problems?

In the longer term, organisations with an information dependency must be prepared to totally replace existing structures and tradition. Perhaps the most difficult paradigm shift will be the recognition that the role of policies, procedures and information systems in preventing information attack today is that they are too often primary *inhibitors* owing to misdirected focus, stopping us dealing with the issues effectively.

It will be necessary for organisations to recognise that the inherent dynamism of information systems may not be amenable to the rigour of traditional organisational control systems. Further, it will not be possible to generalise solutions precisely because of the unfocussed nature of such solutions. Rather, just as the information system configuration itself will dynamically reshape according to the current requirements, so the security configuration and control mechanisms must adapt and evolve through local contextual consideration.

REFERENCES

[1] Hugo Cornwall, 'Datatheft', Heinemann, 1987

[2] Chris Edwards et al, 'Information Technology and the Law', 2nd edition, Macmillan, 1990

[3] Martin Smith, 'Commonsense Computer Security', 2nd edition, McGraw-Hill, 1993

[4] Adrian R. Warman, 'Organisational Computer Security Policies', London School of Economics Working Paper, Department of Information Systems, July 1991

[5] Adrian R. Warman, 'Organisational Computer Security Policies: The Reality', European Journal of Information Systems, Vol. 1, No. 5, pp 305-310, 1992.

[6] James Stoner et al, 'Management', 4th edition, Prentice-Hall, 1989

[7] Andy Reinhardt, 'Building the Data Highway', Byte Magazine, March 1994

[8] Tom Peters, 'Thriving on Chaos: Handbook for a Management Revolution', Pan, 1987

[9] Odd de Presno, 'The Online World', version 1.6, July 1994. This is an electronic book, for further information contact Odd de Presno on opresno@extern.uio.no or presno@grida.no

[10] United States General Accounting Office, 'Computer Security: Government Planning Process Had Limited Impact', Report to the Chairman, Committee on Science, Space, and Technology, House of Representatives, GAO/IMTEC-90-48, 10 May 1990