2006

Organisational Factors and IT Professionals' View of Wireless Network Vulnerability Assessments

Keir Dyce
University of Wollongong, uow_dycek@uow.edu.au

Mary Barrett
University of Wollongong, mbarrett@uow.edu.au

Publication Details

K. Dyce & M. Barrett (2006). Organisational Factors and IT Professionals' View of Wireless Network Vulnerability Assessments. University of Wollongong, First Workshop on the Social Implications of National Security, 29 May.

Organisational Factors and IT Professionals' View of Wireless Network Vulnerability Assessments

Abstract
The paper reports on a survey-based study of Australian computer security professionals' use of and opinions about two types of wireless vulnerability assessment (WNV A): wireless monitoring and penetration testing. An initially surprising finding was how little both types are used, despite the ease with which wireless networks can be attacked, and the lack of clear obstacles to using them.

In the light of aspects of organisational culture, including decision-making style and professional identity, the survey findings become more explicable. Senior management, and even IT staff themselves, may still hold a traditional, 'wired network' view of their organisation. 'Culture' may also explain why lack of time and expertise (rather than lack of financial resources), and senior management's discomfort with the idea of hacking into the network, mean neither wireless monitoring nor penetration testing is regularly used, even though wireless monitoring is fairly well understood.

The paper also explores how aspects of organisational culture may limit the way even WNV A users go about the process, and how a cultural shift could help change users' perception about the risks and rewards of WNV As. This could possibly threaten IT staff's professional identity, however, and this needs further research.

Keywords
view, organisational, factors, network, assessments, professionals, wireless, vulnerability

Disciplines
Business | Social and Behavioral Sciences

Publication Details
K. Dyce & M. Barrett (2006). Organisational Factors and IT Professionals' View of Wireless Network Vulnerability Assessments. University of Wollongong, First Workshop on the Social Implications of National Security, 29 May.

Organisational Factors and Australian IT Professionals' Views of Wireless Network Vulnerability Assessments

Keir Dyce and *Mary Barrett*
Centre for Computer Security Research, School of Management and Marketing
University of Wollongong

Abstract

The paper reports on a survey-based study of Australian computer security professionals' use of and opinions about two types of wireless vulnerability assessment (WNVA): wireless monitoring and penetration testing. An initially surprising finding was how little both types are used, despite the ease with which wireless networks can be attacked, and the lack of clear obstacles to using them.

In the light of aspects of organisational culture, including decision-making style and professional identity, the survey findings become more explicable. Senior management, and even IT staff themselves, may still hold a traditional, 'wired network' view of their organisation. 'Culture' may also explain why lack of time and expertise (rather than lack of financial resources), and senior management's discomfort with the idea of hacking into the network, mean neither wireless monitoring nor penetration testing is regularly used, even though wireless monitoring is fairly well understood.

The paper also explores how aspects of organisational culture may limit the way even WNVA users go about the process, and how a cultural shift could help change users' perception about the risks and rewards of WNVAs. This could possibly threaten IT staff's professional identity, however, and this needs further research.

Keywords: Organisational culture, Wireless network vulnerability assessments, IT professionals, Decision-making style, Professional identity
Discipline: business management>organisational behaviour

Organisational Factors and Australian IT Professionals' Views of Wireless Network Vulnerability Assessments

1 *Introduction*

This paper reports on a study of Australian IT professionals' use of and opinions about wireless network vulnerability assessments (WNVAs) and the organisational factors, especially culture, decision-making and professional identity, which may affect this. Protecting a business organisation's wireless networks presents a classic case of how a technically sophisticated, effective and therefore 'obvious' engineering approach to an important security problem can be undermined by not taking into account its social implications, both inside the organisations where the solutions are implemented, and beyond them.

1.1 *Wireless network security and organisational culture*

For the very reason that the technical solutions to computer security issues appear simple and the need for them clear (at least to those who developed the solutions), their social implications may be difficult for others in the organisation to see, even IT staff. The concepts of organisational culture and especially subculture, that is, the accepted, often unspoken agreements and divisions in 'how we do things around here' go a fair way to explaining why such perceptual divisions are likely to occur and persist within organisations. We will consider culture and subculture from an internal perspective in more detail later in the paper.

Organisational culture is also impacted by the external environment. This has been shown at a broad level by Hofstede's (1980, 1991, 1993) well known studies of national differences in culture. Hofstede's work was undertaken by surveying more than 116,000 IBM employees in more than 40 countries about their work related values. Surveying employees of the same organisation in many countries allowed a variety of national differences in culture to be revealed. Within any one country, social implications of and attitudes towards computer security are likely to be affected by that country's culture. Case researchers such as Spurling (1995), who investigated how the Australian firm Alcoa promoted security awareness and overhauled its security systems, have found evidence suggesting this. Because of the link between external and internal aspects of organisational culture, even IT security professionals' views about computer security may be affected by the anxieties and ambivalences that surround computer security issues in the wider society.

1.2 *Wireless networking, security risk and organisational culture*

As we will see in more detail later, attitudes to risk are a typical part of an organisation's culture. Computer security risk is becoming an increasingly important issue, particularly as applications and uses of wireless network (WLANs) are continuing to develop rapidly in line with the equally rapid development of the 802.11 family of standards and amendments on which the vast majority of wireless networks are based. WLANs enjoy high awareness and acceptance in organisations as they are now fast, cheap and easy to use compared with traditional wired networks. However Housley and Arbaugh (2003) comment that there is as yet a disturbingly low level of security for these networks, especially given that the very nature of wireless transmissions makes it easy to attack them. Specifically, it is easier both to intercept signals during transmission and to 'spoof' fraudulent messages on a wireless network compared to a wired network because the data travelling across a wireless network is transmitted to anyone capable of receiving within range of the signal. Security of information is of course of paramount importance to organisations which use wireless networks. If these networks are left vulnerable, organisations can suffer a whole range of consequences from the trivial and annoying to a potentially shattering organisational blow.

1.3 *Two approaches to wireless network vulnerability assessment*

Wireless network vulnerability assessment (WNVA) is the general term for methods of ensuring that wireless networks are as safe as possible. One kind, wireless monitoring, is a passive approach to testing security measures since it does not involve an attack on a network but rather gathers information about a network that could be put to use in the implementation of an attack – or would allow a network manager to determine if a network has any obvious security flaws. Depending on how it is used wireless monitoring could fall on either side of the boundary of legality or good ethics. Nevertheless a number of security professionals (eg Berghel 2004; Henning 2003; Tiller 2005) see it as an indispensable component in developing a secure wireless network.

A second, complementary approach to wireless network vulnerability assessment is penetration testing (penetration testing), which involves an active attempt to reach the wireless network to test how effective the security measures are in keeping unauthorised users and devices out of the network. It does not involve a full attack on the network, in which an 'attacker' attempts to copy or delete sensitive data and avoid being detected by those responsible for the network. It is a test to see if the wireless network's security measures can be penetrated, and the network accessed.

The issue of wireless security is well covered in a number of texts aimed at security professionals', for example Nichols and Lekkas (2002), Peltier *et al.* (2003) and Tiller (2005). Penetration testing in particular is well understood. However it is not known how widespread WNVA is within organisations. In addition, there is as yet no comprehensive framework outlining how to conduct a comprehensive WNVA. That is, there is no guide involving *both* wireless monitoring and penetration testing approaches which could help IT professionals identify the goals of a vulnerability assessment, prepare for the assessment, actually conduct it, analyse the results, and fix any security flaws that may have been identified. It would be useful to know whether IT professionals would find such a guide helpful. A prototype framework for a WNVA which reflects this lack of integration of the two approaches appears in Figure 1 overleaf.

2 *Finding out IT professionals' use of and views about WNVAs*

A study of what IT professionals actually do and think about WNVAs was conducted via a mail-out survey to members of the Information Security Interest Group (ISIG), an Australian organisation based in Sydney. The ISIG is a group of approximately 400 networking security professionals who were likely to have sole or shared responsibility for the management of one or more 802.11-based wireless networks. The study aimed to clarify some of the problems and unknown elements around IT professionals' use of WNVAs and their views on whether having a comprehensive framework for WNVAs would help them.

The survey contained both closed-ended and open-ended questions, giving respondents the opportunity to include additional information or opinion on specific issues. The study did not aim to link one variable causally with another, nor did it try to identify correlations between two or more variables, for example to try to connect views about WNVA issues with aspects of the IT professionals themselves or their organisations. Nevertheless the surprising nature of some of the results and the patterns in them suggest that some organisational factors, especially aspects of organisational culture and issues around IT professionals' identity, may have influenced the results. The results and discussion of these potential organisational factors, are presented under the three main headings of the survey itself:

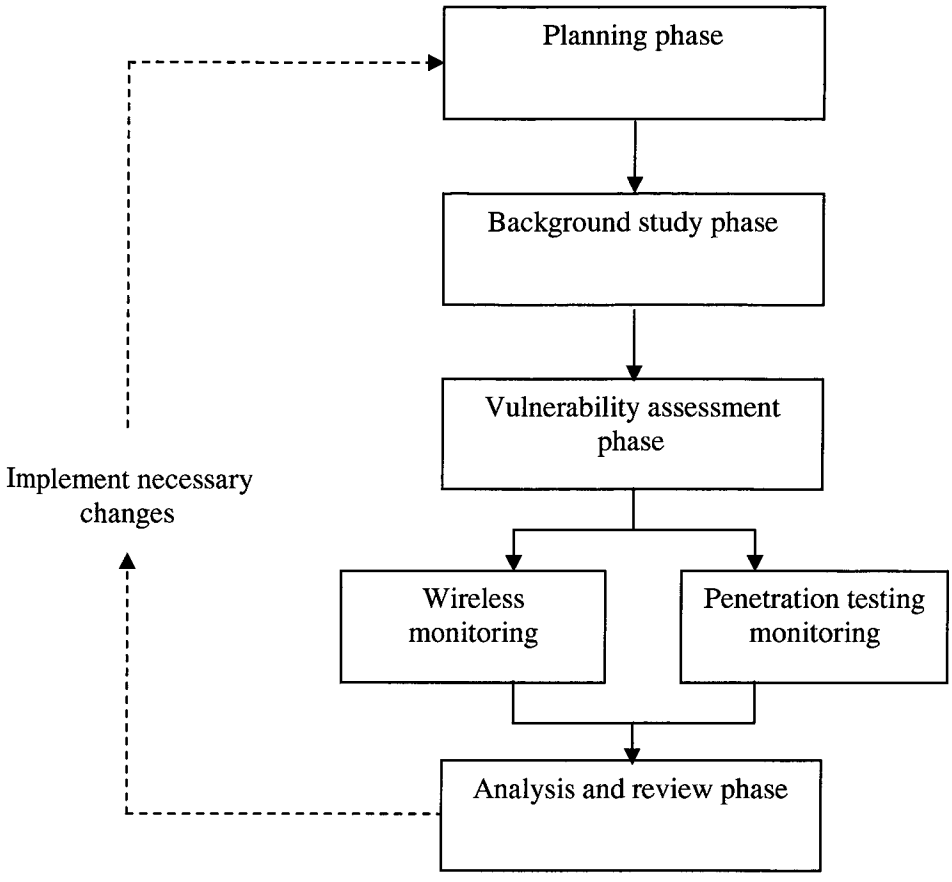

Figure 1: Prototype vulnerability assessment framework

1. the extent of use of WNVAs, including either or both wireless monitoring and penetration testing,

2. how IT professionals used WNVAs, and

3. their opinions about the two approaches to WNVAs, and about aspects of vulnerability assessment frameworks.

3 *Results*

3.1 *Use of vulnerability assessments*

A total of 62 useable survey responses were received. This appears a modest result, but given that the organisation consists of only about 400 members, the responses can be assumed to provide a reasonable view of the group whose views were sought.

Of the 62 respondents, only ten (16 percent) said they used wireless monitoring and three (5 percent) used penetration testing. This was a surprisingly low result, especially for wireless monitoring, which is widely known and publicised amongst IT professionals. The most common reason given in for not using wireless monitoring and penetration testing was that they were felt unnecessary. The second most common reason was a perceived lack of the necessary expertise for the two kinds of testing. Interestingly, lack of resources or other reasons were *not* perceived to be the problem.

3.1.1 *Discussion: The possible role of organisational culture*

When possible organisational factors are considered, however, especially organisational culture, it is less surprising that WNVAs have yet to find acceptance within organisations, even among IT professionals. Organisational culture encompasses such issues as the degree to which employees are expected to pay attention to detail and to results, and be aggressive and competitive. It also includes the degree to which organisations are oriented around people's needs, rely on teams to organise work, and emphasise stability rather than growth (O'Reilly, Chatman & Caldwell 1991). An organisation's culture is known to be strongly influenced by senior management's style and preferences, the organisation's work and communication practices, reward structures, past history, power relationships, customer or user demands, accepted explanations of competitive pressures, and so on (Schein 1985). Culture serves as a powerful, practical and yet tacit way of organising management and employees' (including IT staff's) knowledge of the organisation's priorities and ways of operating.

Cultural values and assumptions, which are embedded at a deep level, sometimes remain when circumstances have changed, inhibiting the organisation's ability to respond to change. Thus earlier cultural norms about organisational security may outweigh IT professionals' judgements or even awareness of the need to revise standard security measures. We could predict, for example, that WNVAs would not be seen as necessary, since powerful organisational stakeholders including senior management, and even IT staff themselves, may still hold a traditional, 'wired network' view of their organisation, even though this is now more a part of history than reality. Many of the vulnerability assessment frameworks currently available are also based on the assumption that they will be applied in a wired rather than a wireless environment (Dyce 2005). This would tend to entrench the existing security norms of many organisations.

As the O'Reilly, Chatman & Caldwell (1991) formulation of cultural elements suggests, aspects of organisational culture strongly influence perceptions of what is important to organisational success. So culture also tends to dictate the choice of matters organisational members see as worthy of their time and effort. This may help explain why lack of time and expertise (rather than lack of financial resources), as well as senior management's discomfort with both the idea of hacking into the network, mean neither wireless monitoring nor penetration testing were regularly used.

3.1.2 *Dominant cultures and subcultures*

These explanations relate to views of the dominant organisational culture, generally the one espoused by senior management. However researchers on organisational culture such as Jermier *et al.* (1991) and Sackmann (1992) also point to the existence in most sizeable organisations of one or more subcultures which may or may not work in the same direction as the dominant organisational culture. Senior management, who as non-IT experts are unlikely to know much about the technical detail of WNVAs, may assume penetration testing involves hacking into the network, actually deleting data and then concealing the attack. IT security staff, by contrast, would most likely know that merely showing that a potential intruder could access the network is all penetration testing actually requires. If this is true, and it would be useful to undertake further research to establish the point, the dominant culture could be behind the lack of use of penetration testing.

By contrast, the IT subculture alone or in combination with the dominant culture may well be behind the non-use of wireless monitoring. As noted earlier, wireless monitoring can be used for illegal and/or unethical activity, such as monitoring which invades the privacy of employees or other parties. IT staff may therefore be concerned that using wireless monitoring may cause them as a group to be perceived by other organisational members as instigating inappropriate monitoring practices. Senior managers may be less concerned about

this perception. After all many large organisations already monitor employees' web use and have told them this. However they may still be concerned about implementing new, possibly unpopular monitoring practices unless there is an overwhelming and demonstrated need to do so. In this case the dominant and the IT sub-culture may work together to discourage use of wireless monitoring.

3.2 *How WNVAs are used*

The answers to this section of the questionnaire broadly indicated that of the ten WNVA users in the sample, most had found that using either wireless monitoring or penetration testing or a combination of the two had proved valuable, in that network vulnerabilities had been revealed. A range of vulnerabilities had been both tested for and found, the latter ranging from incorrect security configurations, rogue WAPs, overextended network boundaries and newly publicised vulnerabilities. A majority of those in the sample who used WNVA also indicated that one or other or both of wireless monitoring and penetration testing were part of the standard security procedures in their organisations. The results of a question about what practices are used as part of standard security procedure indicated that six of the ten WNVA users used just wireless monitoring, none used just penetration testing, and three used both. It was rare however to find that both wireless monitoring and penetration testing were used simultaneously in an organisation.

3.2.1 *Discussion*

In an earlier part of the results, thirty respondents or about half the sample said they believed a WNVA framework would help those who don't use either wireless monitoring or penetration testing due to lack of expertise. Moreover, the experience of WNVA users suggests that WNVAs are proving useful to organisations, and that users themselves recognise the value of making a WNVA a consistent procedure. The gap between the two findings – thirty respondents who believe a WNVA framework could be helpful for those who lack expertise, and only ten actual users – suggests that the lack of good WNVA frameworks may be preventing IT staff from implementing WNVAs. The next section explores this possibility further.

3.3 *Practitioners' opinions about WNVAs including WNVA frameworks*

In light of the findings about how WNVAs are used, it was surprising that practically all ten respondents who used WNVAs said they did not use a framework or a methodology to help them conduct security procedures. Three of the ten used a wireless monitoring framework; two of the ten used a penetration testing framework. Seven of the ten considered planning to be valuable as part of WNVAs, but only one had researched what approach to use. Very few used a framework (or knew where they could find one) for setting up, evaluating or refining a WNVA exercise. In addition, very few felt a WNVA should be done routinely after network changes, despite the fact that such changes may introduce network vulnerabilities.

3.3.1 *Discussion – the possible role of organisational decision-making style*

IT professionals using WNVAs have found them useful and incorporated them into standard operating procedures. At first glance, this makes it surprising that very few IT professionals in this sample used of any framework to carry out a WNVA. However styles of organisational decision-making may explain this situation. Styles of decision-making, whether slow and considered, or fast and impulsive, also form part of culture. 'Planning' will fit with espoused values of rationality in most organisations' cultures, and also with cultures which are 'outcomes' rather than 'process' focussed. According to Simon (1979), however, in practice it is often impossible to explore planning options exhaustively because of time constraints and other limitations of the working environment. Instead, people typically use what he has called

'bounded' decision-making. That is, they make decisions on the base of limited research and choose from a reduced number of options. Because a limited range of options has been explored, bounded decision-making may lead to less than optimal results.

The absence of a well known and established WNVA framework could explain why most of the ten WNVA users would report that they endorse 'planning' in WNVAs but actually make little or no use of planning frameworks. The amount of time and expertise needed to find an appropriate framework, and then seek support for its use from senior management or other areas of the organisation, could discourage even those who claim to plan their WNVAs. The easier alternative would be to use no framework, and also carry out the WNVA without informing other organisational members. The time needed both to find and gain support for a procedure which other parts of the organisation are likely to misunderstand and mistrust, as well the fear of hacking mentioned earlier, could explain the finding that the majority of WNVAs users preferred that other organisational members not know that vulnerability assessments are used. As Takanen *et al.* (2004) have argued in their discussion of the distributions of responsibility among various actors in software vulnerability situations, this could compromise the ethical standards of the IT staff carrying out the procedure.

4 *Conclusions*

Organisational culture – especially because of its link with concerns in the wider society – may explain why IT professionals typically don't use either kind of WNVA or even seem to know about them. Wireless monitoring, as we have seen, entails surveillance of human activity on an important aspect of an organisation's infrastructure: its networks. On the one hand, as a population, we are becoming used to surveillance. We are being watched more than ever before, via cameras at shopping centres, e-tags in tunnels, and a vast range of electronic transactions. A lot of the time we are not bothered by this, and overlook how much surveillance is being done. An example of this 'aware and yet not aware' attitude is demonstrated in how a recent murder conviction in an Australian capital city was secured. The perpetrator claimed he was asleep at home in another city at the time of the crime, but evidence obtained from e-tag data – a form of daily surveillance that inner city drivers know about but forget – showed his car had been moving towards the victim's location shortly beforehand.

So we are often relaxed, 'knowing but unknowing', about surveillance. It is becoming part of our culture both in our organisations and outside them. However we are typically less sanguine when it is pointed out how much surveillance we are being subjected to. Australians have so far rejected smart identity cards, perhaps feeling that their convenience would be outweighed by increased surveillance they might lead to. Wireless monitoring, because it involves surveillance, could well create this ambivalence on the part of non IT staff. Even computer security staff may be ambivalent about wireless monitoring because of their concerns about how other organisational members will perceive them. Vulnerability assessments using penetration testing, with its overtones of an attack, could create even more anxiety. Again, while computer security staff may know that no real attack will happen, they may dislike being regarded by others as something akin to a hacker and having to explain their role. In short, employees, including IT staff, live in the external world as well as the world of their organisations. So while they are likely to see the need for computer security they may also be ambivalent about what they have to do to achieve it.

5 *Recommendations*

According to Dunphy and Stace (1993), dealing with the effects of organisational culture involves either living within the culture as it is and making the most of its positive aspects, or trying to change the culture.

5.1 *Improving organisational security within the existing organisational culture*

The implications for businesses wanting to improve their computer security are that they need to take account of how aspects of organisational culture may work against computer security as well as for it. With respect to wireless network security, they need to be aware of the anxieties – both internal and external – that are likely to be associated with WNVAs. Businesses have always needed to be mindful of how their activities are perceived by both their external and internal 'publics'. The difficulties of Enron, Shell, the Australian Wheat Board, James Hardie and many other firms which have been accused of poor behaviour, are due in part to what people – insiders as well as outsiders – believed they *could* do as well as what they actually *did* do. Living with this situation, as XXX has shown, requires frequent and credible communication with the organisation's internal and external publics about why specific security strategies are necessary.

5.2 Improving organisational security by changing organisational culture

Tacit knowledge as embodied in organisational culture may be altered, although this is typically difficult and time-consuming. Various approaches to changing organisational culture in the interests of helping the organisation adapt to other necessary change have been examined by change theorists such as Argyris (1990), Dunphy and Dick (1981), Dunphy and Stace (1993), Kotter (1995) and Lewin (1951). These theorists all argue that specific changes should be embedded into the organisation's culture. Introducing a new security protocol would be an apt example of a change requiring this treatment. Embedding change into culture is typically the last and most difficult part of a planned change process, though often the most important if the change is to remain. A major computer security breach or the threat of one may be sufficient to establish a sense of critical urgency needed to convince organisational members of the need to do things differently. This is the first step in most theorists' recommendations for successful planned change.

Embedding WNVAs into organisational culture could be helped by incorporating them, and an appropriate framework for carrying them out, into standard operating procedures. To apply Schein's ideas about the importance of organisational stories and rituals in transmitting and embedding aspects of culture, organisational stories about security breaches detected and harm avoided, preferably without damage to other employees' privacy and with appropriate rewards allocated, could over the long term change users' perceptions about the risks and rewards of WNVAs.

Such cultural change is unlikely to happen without problems. The necessary cultural shifts may well threaten aspects of ICT professionals' work identity, for example, since subcultures including those of IT professionals have been shown to depend in part on their special expertise which contributes to the power they can exercise in organisations (Jermier *et al.* 1991; Sackman 1992). This and other implications of the results of the present study, for example in the areas of IT professional ethics, computer security awareness education, and so on, requires further research.

6 *References*

Anonymous (2003) 'Wireless networks grow dramatically, but security remains a problem, report says', *Electronic Commerce News*, **8** (31 March).

Argyris, C. (1990) *Overcoming Organizational Defenses*. Boston: Allyn and Bacon.

Berghel, H. and Uecker J. (2004) 'Wireless Infidelity I: War Driving', *Communications of the ACM*, **47** (9), pp. 21-26.

Dunphy, D. and Dick, R. (1981) *Organizational Change by Choice.* Sydney, New York: McGraw-Hill.

Dunphy, D. and Stace, D. (1993) 'The Strategic Management of Corporate Change', *Human Relations*, **46** (8), pp. 905-20.

Dyce, K. (2005) *A Wireless Vulnerability Assessment Framework: A developed prototype wireless vulnerability assessment framework and a study into their use in the real world.* Unpublished Honours thesis, University of Wollongong.

Henning, R. R. (2003) *Vulnerability Assessment in Wireless Networks*, Harris Corporation, [Available Online: http://www.cs.nmt.edu/~cs553/paper15.pdf], Accessed 5 January 2006.

Hofstede, G. (1980) *Culture's Consequences: International Differences in Work Related Values*, Beverly Hills: Sage.

Hofstede, G. (1991) *Cultures and Organizations: Software of the Mind*, London: McGraw-Hill.

Hofstede, G. (1993) 'Cultural Constraints in Management Theories', *Academy of Management Executive*, (**February**), pp. 81-94.

Housley, R. and Arbaugh, W. (2003) 'Security Problems in 802.11-based Networks', *Communications of the ACM*, **46** (5) (May), pp. 31-34.

Jermier, J. M., Slocum, J. W., Fry, L. W. and Gaines, J. (1991) 'Organizational Subcultures in a Soft Bureaucracy: Resistance Behind the Myth and Façade of an Official Culture', *Organizational Science*, (May), pp. 170-94.

Kotter, J. P. (1995) 'Leading Change: Why Transformational Efforts Fail', *Harvard Business Review*, **73** (March-April), pp. 59-67.

Lewin, K. (1951) *Field Theory in Social Science.* New York: Harper and Row.

O'Reilly III, C. A., Chatman, J. and Caldwell, D. F. (1991) 'People and Organizational Culture: A Profile Comparison Approach to Assessment of Person-Organization Fit', *Academy of Management Journal*, (**September**), pp. 487-516.

Nichols, R. K. and Lekkas, P. C. (2002) *Wireless Security: Models, Threats and Solutions*, New York: McGraw-Hill.

Peltier, T. R., Peltier, J. and Blackley, J. A. (2003) *Managing a Network Vulnerability Assessment*, Auerbach Publications, USA.

Sackmann, S. A. (1992) 'Culture and Subcultures: an Analysis of Organizational knowledge', *Administrative Science Quarterly*, (**March**), pp. 140-61.

Schein, E. H. (1985) *Organizational Culture and Leadership.* San Francisco, CA: Jossey Bass.

Schein, E. H. (1993) 'On Dialogue, Culture, and Organizational Learning', *Organizational Dynamics*, (Winter), pp. 40-51.

Simon, Herbert A.. (1979) 'Rational Decision Making in Business Organizations', *American Economic Review*, **69** (4), pp. 493-513.

Spurling, P. (1995) 'Promoting security awareness and commitment', *Information Management & Computer Security*, **3** (2), pp. 20-26.

Takanen, A., Vuorijärvi, P., Laakso, M. and Röning, J. (2004) 'Agents of responsibility in software vulnerability processes', in *Ethics and Information Technology*, **6**, pp. 93-110.

Tiller, J. S. (2005) *The Ethical Hack: A Framework for Business Value Penetration Testing*, Auerbach Publications, USA.