



Journal of Theoretical and Applied Electronic
Commerce Research

E-ISSN: 0718-1876

ncerpa@utalca.cl

Universidad de Talca
Chile

Dyce, Keir; Barrett, Mary

Taking Care of (E)-Business?: Australian IT Professionals' Views of Wireless Network Vulnerability
Assessments

Journal of Theoretical and Applied Electronic Commerce Research, vol. 1, núm. 2, august, 2006, pp.
79-89

Universidad de Talca
Curicó, Chile

Available in: <http://www.redalyc.org/articulo.oa?id=96510208>

- How to cite
- Complete issue
- More information about this article
- Journal's homepage in redalyc.org

redalyc.org

Scientific Information System

Network of Scientific Journals from Latin America, the Caribbean, Spain and Portugal

Non-profit academic project, developed under the open access initiative

Taking Care of (E)-Business?: Australian IT Professionals' Views of Wireless Network Vulnerability Assessments

Keir Dyce¹ and Mary Barrett²

¹Centre for Computer Security Research, University of Wollongong, Wollongong, Australia kfd42@uow.edu.au

²Centre for Leadership and Knowledge Management, School of Management and Marketing, University of Wollongong, Wollongong, Australia mbarrett@uow.edu.au

Received 05 December 2005; received in revised form 08 May 2006; accepted 30 June 2006

Abstract

M-commerce, a growing sub-category of E-business, allows business to be done 'anywhere, anytime'. However security of wireless devices remains problematic. It is unclear whether protocols to alleviate security problems, such as wireless vulnerability assessments (WNVAs), are being used or are effective. The paper reports on a survey-based study of Australian computer security professionals' use of and opinions about two types of 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 fact that penetration testing is fairly well understood. In the light of organizational culture the survey findings become more explicable. Senior management, and even IT staff, may still hold a traditional, 'wired network' view of their organization. Aspects of organizational culture also appear to limit the way WNVA users go about the assessment process. A cultural shift could help change users' perceptions about the risks and rewards of WNVAs. This could threaten IT staff's professional identity, however, and needs further research.

Key words: organizational culture, wireless network vulnerability assessment, computer security, m-commerce

1 Introduction

Recent technological advances in mobile devices and wireless networks mean increasing use of wireless devices for e-commerce purposes. M-commerce applications, as they are sometimes called to distinguish them from the broader field of online or e-commerce applications, share the advantages of ubiquity, convenience, accessibility, personalization and localization [4]. Mobile users can now order goods in an anywhere and anytime fashion. Quality of service issues are being overcome through technical improvements such as better bandwidth provision to eliminate loss of service between mobile users [2]. This could be expected to add to wireless devices' attractiveness for m-commerce. However, studies of user perceptions of mobile and online channels have found business users are reluctant to use m-commerce technologies for 'risky' transactions such as purchasing or investment [23], [24].

Clearly, security remains a major and under-researched issue with wireless technologies [24]. At an organizational level, business-related or otherwise, wireless network vulnerability assessments (WNVAs) could be expected to be part of the normal security protocols to protect B2B transactions. However, despite general awareness that m-commerce devices are insecure, little is known about how much confidence IT professionals place in WNVAs or even how much they use them. This paper reports on a study of Australian IT professionals' use of and opinions about wireless network vulnerability assessments (WNVAs) and the organizational factors, especially culture, decision-making and professional identity, which may affect this. Protecting a business organization'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 organizations where the solutions are implemented, and beyond them.

1.1 Wireless Network Security and Organizational 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 organization to see, even IT staff. The concepts of organizational culture and especially subculture, that is, the accepted, often unspoken agreements and divisions in 'how we do things around here', do much to explain why such perceptual divisions are likely to occur and persist within organizations. We will consider culture and subculture from an internal perspective in more detail later in the paper.

Organizational culture is also affected by the external environment. This has been shown at a broad level by Hofstede's well known studies of national differences in culture [9], [10], [11]. 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 organization 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 research, e.g. of how the Australian firm Alcoa promoted security awareness and overhauled its security systems, strongly suggests this [22]. Because of the link between external and internal aspects of organizational 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 Organizational Culture

As we will see in more detail later, attitudes to risk are a typical part of an organization'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 organizations as they are now fast, cheap and easy to use compared with traditional wired networks. However there is as yet a disturbingly low level of security for these networks; in fact the very nature of wireless transmissions makes it easy to attack them [12]. 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 traveling across a wireless network is transmitted to anyone capable of receiving within range of the signal. Security of information is of paramount importance to organizations which use wireless networks. If these networks are left vulnerable, organizations can suffer a whole range of consequences from the trivial and annoying to a potentially shattering organizational 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 many security professionals see it as an indispensable component in developing a secure wireless network [3], [8], [25].

A second, complementary approach to wireless network vulnerability assessment is penetration testing, which involves an active attempt to reach the wireless network to test how effective the security measures are in keeping unauthorized 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 [16], [18], [25]. Penetration testing in particular is well understood. However it is not known how widespread WNVA is within organizations. 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, analyze 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.

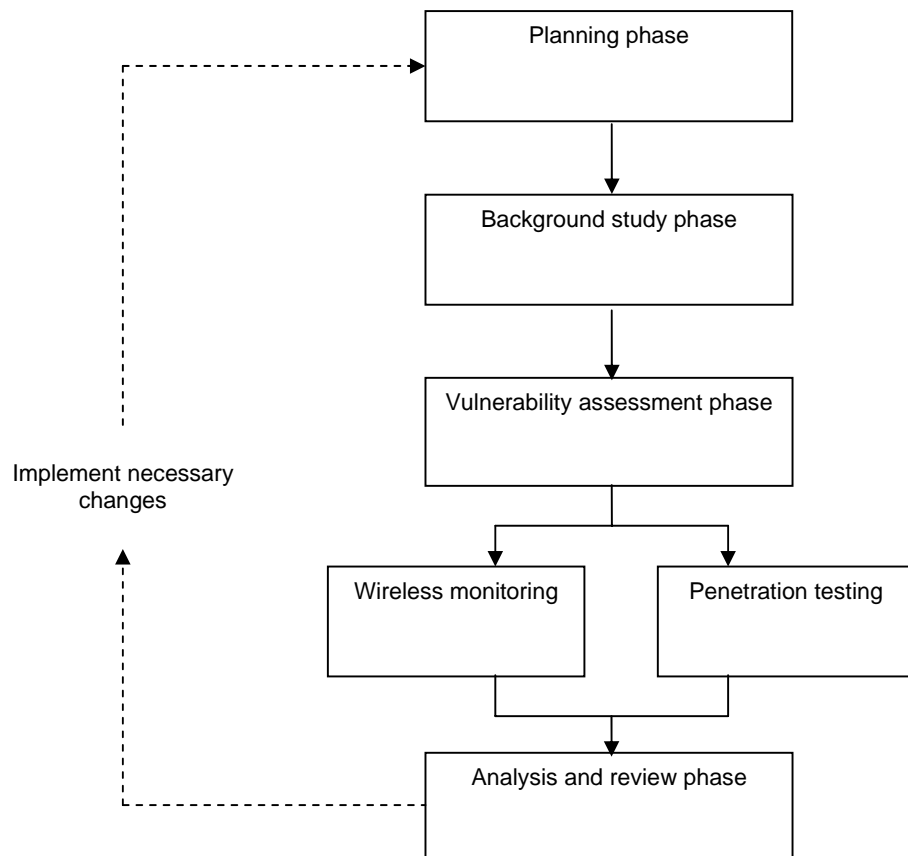


Figure 1: Prototype vulnerability assessment framework

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 organization based in Sydney, Australia. 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. Table 1 shows the organizational roles of ISIG members. Members are typically aged between 35 and 50 years. As the Table indicates, the percentage of technically focused security staff compared to staff in sales, management or consultancy roles is low, making this an appropriate group to study to IT professionals' views.

Area	Percent
Management	30
Consultancy	30
Sales	25
Technical	15

Table 1: IT Security Roles of ISIG members
(Source: ISIG Australia)

The survey contained both closed-ended and open-ended questions, giving respondents the opportunity to include additional information or opinion on specific issues. See survey instrument used in the study appears in the Appendix. 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 organizations. Nevertheless the surprising nature of some of the results and the patterns in them suggest that some organizational factors, especially aspects of organizational culture and issues around IT professionals' identity, may have influenced the results. The results and discussion of these potential organizational factors are presented under the three main headings of the survey itself:

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 organization 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 publicized amongst IT professionals. The most common reason given 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.

Discussion: The Possible Role of Organizational Culture

When possible organizational factors are considered, especially organizational culture, it is less surprising that WNVAs have yet to find acceptance within organizations, even among IT professionals. Organizational 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 organizations are oriented around people's needs, rely on teams to organize work, and emphasize stability rather than growth [17]. An organization's culture is known to be strongly

influenced by senior management's style and preferences, the organization's work and communication practices, reward structures, past history, power relationships, customer or user demands, accepted explanations of competitive pressures, and so on [20]. Culture serves as a powerful, practical and yet tacit way of organizing management and employees' (including IT staff's) knowledge of the organization'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 organization's ability to respond to change. Thus earlier cultural norms about organizational security may outweigh IT professionals' judgments 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 organizational stakeholders including senior management, and even IT staff themselves, may still hold a traditional, 'wired network' view of their organization, 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 [7]. This would tend to entrench the existing security norms of many organizations.

As the formulation of cultural elements in [17] suggests, aspects of organizational culture strongly influence perceptions of what is important to organizational success. So culture also tends to dictate the choice of matters organizational 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.

Dominant Cultures and Subcultures

These explanations relate to views of the dominant organizational culture, generally the one espoused by senior management. However researchers on organizational culture [13], [19] also point to the existence in most sizeable organizations of one or more subcultures which may or may not work in the same direction as the dominant organizational 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 explain 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 organizational members as instigating inappropriate monitoring practices. Senior managers may be less concerned about this perception. After all many large organizations 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 publicized vulnerabilities. A majority of those in the sample who used WNVA also indicated that either or both of wireless monitoring and penetration testing were part of the standard security procedures in their organizations. 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 organization.

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 organizations, and that users themselves recognize 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 and 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.

Discussion: The Possible Role of Organizational 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 any framework to carry out a WNVA. However styles of organizational 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 organizations' cultures. Planning will also fit easily into cultures which are 'outcomes' rather than 'process' focused. In practice, however, 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 Simon has called 'bounded' decision-making. That is, decision-makers choose options on the basis of limited research and a limited range of possibilities. As a result, bounded decision-making may lead to less than optimal results [21].

The absence of a well known and established WNVA framework could explain why most of the ten WNVA users reported 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 organization, 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 organizational members. The time needed both to find and gain support for a procedure which other parts of the organization 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 organizational members not know that vulnerability assessments are used. Research into the distributions of responsibility among various actors in software vulnerability situations suggests this could compromise the ethical standards of the IT staff carrying out the procedure.

4 Conclusions

Organizational 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 organization'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 centers, 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 organizations 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 organizational 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 organizations. 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 [6], dealing with the effects of organizational 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 Organizational Security Within the Existing Organizational Culture

The implications for businesses wanting to improve their computer security are that they need to take account of how aspects of organizational 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 behavior, 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 requires frequent and credible communication with the organization's internal and external publics about why specific security strategies are necessary [22].

5.2 Improving Organizational Security by Changing Organizational Culture

Tacit knowledge as embodied in organizational culture may be altered, although this is typically difficult and time-consuming. Various approaches to changing organizational culture in the interests of helping the organization adapt to other necessary change have been examined by change theorists [1], [5], [6], [14], [15]. These theorists all argue that important changes should be embedded into the organization's culture to be successful. 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 organizational members of the need to do things differently. This is the first step in most theorists' recommendations for successful planned change.

Embedding WNVAs into organizational culture could be helped by incorporating them, and an appropriate framework for carrying them out, into standard operating procedures. Change theorists endorse telling organizational stories and developing rituals to transmit and embed aspects of culture [1], [5], [6], [14], [15]. Accordingly, developing and telling organizational 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 organizations [13], [19]. 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.

Acknowledgment

Keir Dyce and Mary Barrett would like to acknowledge the assistance of Professor Jennifer Seberry, Director of the Centre for Computer Security Research at the University of Wollongong, who was the supervisor of the Honors project which led to this paper.

References

- [1] C. Argyris, *Overcoming Organizational Defenses*. Boston: Allyn and Bacon, 1990.
- [2] I. Awan and S. Singh, Performance Evaluation of E-commerce Requests in Wireless Cellular Networks, *Information and Software Technology*, vol. 48, no. 6, pp. 393-401, 2006.
- [3] H. Berghel and J. Uecker, Wireless Infidelity I: War Driving, *Communications of the ACM*, vol. 47, no. 9, pp. 21-26, 2004.
- [4] X. Ding, J. Iijima, and S. Ho, Unique Features of Mobile Commerce, *Journal of Electronic Technology of China*, vol. 2, no. 3, pp. 205-210, 2004.
- [5] D. Dunphy and R. Dick, *Organizational Change by Choice*. Sydney, New York: McGraw-Hill, 1981.
- [6] D. Dunphy and D. Stace, The Strategic Management of Corporate Change, *Human Relations*, vol. 46, no. 8, pp. 905-920, 1993.

- [7] K. Dyce, A Wireless Vulnerability Assessment Framework: A developed prototype wireless vulnerability assessment framework and a study into their use in the real world. Honors thesis, School of Information Technology and Computer Science, University of Wollongong, Wollongong, Australia, 2005.
- [8] R. R. Henning. (2003). Vulnerability Assessment in Wireless Networks. Harris Corporation. [Online]. Available: <http://www.cs.nmt.edu/~cs553/paper15.pdf>.
- [9] G. Hofstede, Culture's Consequences: International Differences in Work Related Values. Beverly Hills: Sage, 1980.
- [10] G. Hofstede, Cultures and Organizations: Software of the Mind. London: McGraw-Hill, 1991.
- [11] G. Hofstede, Cultural Constraints in Management Theories, Academy of Management Executive, vol. 7, no. 1, pp. 81-94, 1993.
- [12] R. Housley and W. Arbaugh, Security Problems in 802.11-based Networks, Communications of the ACM, vol. 46, no. 5, pp. 31-34, 2003.
- [13] J. M. Jermier, J. W. Slocum, L. W. Fry, and J. Gaines, Organizational Subcultures in a Soft Bureaucracy: Resistance Behind the Myth and Façade of an Official Culture, Organizational Science, vol. 2, pp. 170-194, 1991.
- [14] J. P. Kotter, Leading Change: Why Transformational Efforts Fail, Harvard Business Review, vol. 73, (March-April), pp. 59-67, 1995.
- [15] K. Lewin, Field Theory in Social Science. New York: Harper and Row, 1951.
- [16] R. K. Nichols and P. D. Lekkas, Wireless Security: Models, Threats and Solutions, New York: McGraw-Hill, 2002.
- [17] C. A. O'Reilly III, J. Chatman, and D. F. Caldwell, People and Organizational Culture: A Profile Comparison Approach to Assessment of Person-Organization Fit, Academy of Management Journal, vol. 34, pp. 487-516, 1991.
- [18] T. R. Peltier, J. Peltier, and J. A. Blackley, Managing a Network Vulnerability Assessment. Auerbach Publications, 2003.
- [19] S. A. Sackmann, Culture and Subcultures: An Analysis of Organizational Knowledge, Administrative Science Quarterly, vol. 37, pp. 140-161, 1992.
- [20] E. H. Schein, Organizational Culture and Leadership, San Francisco, CA: Jossey Bass, 1985.
- [21] H. A. Simon, Rational Decision Making in Business Organizations, American Economic Review, vol. 69, no. 4, pp. 493-513, 1979.
- [22] P. Spurling, Promoting security awareness and commitment, Information Management & Computer Security, vol. 3, no. 2, pp. 20-26, 1995.
- [23] T. J. Strader and Sridhar N. Ramaswami, Investor Perceptions of Traditional and Online Channels, Communications of the ACM, vol. 47, no. 7, pp. 73-76, 2004.
- [24] T. J. Strader, P. Tarasewich, and R. Nickerson, The state of wireless information systems and mobile commerce research, Information Systems and E-Business Management, vol. 2, no. 4, pp. 287-292, 2004.
- [25] J. S. Tiller, The Ethical Hack: A Framework for Business Value Penetration Testing, Auerbach Publications, 2005.

Appendix: Survey Instrument Used in the Study

Section 1: The Prevalence of Use of Vulnerability Assessments

1 Do you or your organization conduct **wireless monitoring** (as per the given definition) on a wireless local area network (WLAN)?

Yes No Don't know No response

2 If you answered '**No**' to question 1, what is the main reason for not conducting wireless monitoring on your/the organization's WLAN?

Not considered necessary Not considered worthwhile Lack of necessary expertise Lack of resources (time, money, equipment) Other No response

3 Do you or your organization conduct **penetration testing** (as per the given definition) on a wireless local area network?

Yes No Don't know No response

4 If you answered '**No**' to question 3, what is the main reason for not conducting penetration testing on your/the organization's WLAN?

Not considered necessary Not considered worthwhile Lack of necessary expertise Lack of resources (time, money, equipment) Other No response

5 If you answered 'Lack of necessary expertise' to question 2 **OR** 4, would a framework/methodology that would guide you through the necessary steps make conducting wireless monitoring or penetration testing more appealing?

Yes No Don't know No response

Section 2: How Vulnerability Assessments are Used by Practitioners

6 How often do you/your organization conduct **wireless monitoring** on the WLAN?

Once a month, or more often Once every 1-3 months Once every 3-6 months Once every 6-12 months Conducted it only once Don't know No response

7 How often do you/your organization conduct **penetration testing** on the WLAN?

8 Is the practice of conducting wireless monitoring and/or penetration testing part of a set security practice?

Just wireless monitoring Just penetration testing Both wireless monitoring and penetration testing Don't know No response

9 Do you/your organization conduct wireless monitoring and penetration testing at the same time?

Yes, all the time No Sometimes Don't know No response

10 Has the practice of wireless monitoring detected security vulnerabilities (such as role/unauthorized access points, improper WLAN security configuration, etc?)

Yes No Don't know No response

11 Has the practice of penetration testing helped you identify how difficult it would be for a hacker to gain access to the WLAN?

Yes No Don't know No response

12 If you answered '**Yes**' to either question 10 **OR** 11, please indicate the types of vulnerability detected, if known:

Yes No Don't know No response

13 If, after implementing changes to the configuration of the WLAN (security or otherwise), do you conduct a vulnerability assessment to test the security of the changes?

Yes, all the time No Sometimes Don't know No response

14 If you define objectives/goals for the vulnerability assessment what is the most common goal?

Checking the security configuration of the WLAN
Testing for rogue wireless access points
Checking if a network configuration change has impacted on security
Testing how difficult it is for a hacker to gain access to the WLAN
Testing if the WLAN suffers from a known vulnerability
Other
No response

Section 3: Use and Opinions Regarding Vulnerability Assessment Frameworks

15 Do you/your organization follow a methodology or framework for conducting wireless monitoring on the wireless local area network? Or do you conduct it in an ad hoc manner?

Framework/Methodology Ad hoc Don't know No response

16 Do you/your organization follow a methodology or framework for conducting penetration testing on the WLAN? Or do you conduct it in an ad hoc manner?

Framework/Methodology Ad hoc Don't know No response

17 If you answered '**Ad hoc**' to question 15 **OR** 16, do you plan the vulnerability assessment before you begin (such as the objectives of the test, what will be tested, etc)?

Yes, all the time No Sometimes Don't know No response

18 Do you consider planning a valuable aspect of conducting a vulnerability assessment?

Yes No Don't know No response

19 Please give a brief statement about why or why not you consider planning to be important:

20 If you answered '**Framework/Methodology**' to questions 15 **OR** 16 above is it a framework/methodology developed by yourself or someone within your organization?

Developed Developed Don't know No response
in-house externally

21 If no, is it one sourced from a publication (such as a journal, book etc), another organization or from another source?

A publication An organization Other Don't know No response

22 If you/your organization conducts **wireless monitoring** on your/its WLANs, has it proven to be a useful practice?

Yes No Don't know No response

23 If you/your organization conducts **penetration testing** on your/its WLANs, has it proven to be a useful practice?

Yes No Don't know No response

24 Do you feel it is important to review the vulnerability assessment in order to refine the testing process? (e/g/ What went well? What didn't go well? What could be improved)? If you/your organization conducts **wireless monitoring** on your/its WLANs, has it proven to be a useful practice?

Yes No Don't know No response

25 Do you feel that vulnerability assessments should be an almost continuous process (in order to test whether changes made to fix the vulnerabilities detected in a previous vulnerability assessment were successful)? If you/your organization conducts **wireless monitoring** on your/its WLANs, has it proven to be a useful practice?

Yes No Don't know No response

26 Do you feel it is or would be useful to conduct the test in as real a situation as possible in order to recreate the conditions a potential intruder would operate under (for example, by conducting the vulnerability assessment from outside the building)? If you/your organization conducts **wireless monitoring** on your/its WLANs, has it proven to be a useful practice?

Yes No Don't know No response

27 Do you inform users of the WLAN that is to be subject to a vulnerability assessment of the assessment?

Yes No, it is not No, I believe users should not be Sometimes No response
worthwhile aware of the coming assessment

28 Do you conduct research or a background study to gather information before you commence an actual vulnerability assessment (e.g. existing WLAN security policy document, results from previous vulnerability assessments, WLAN configuration document, information on recently announced vulnerabilities)?

Yes, always No Sometimes Don't know No response

29 What, if any, are the problems you have come across while conducting a vulnerability assessment on a wireless network? Please give details of any problems.

30 Finally, do you have any other general comments about conducting vulnerability assessments on WLANs?