The Influence of Institutional Forces on Employee Compliance with Information Security Policies

Ye Hou, Ping Gao and Richard Heeks

The University of Manchester, Manchester, U.K.

Abstract. Information Security is an issue of growing concern to organisations, typically addressed by development of information security policies. However, policies are only effective if organizational employees comply with them. This paper reviews literature related to employees' security behaviour and information security policy compliance and presents research gaps from literature review on influencing employees' compliance behaviour with information security policy. Here, we analyse the institutional factors that shape employee behaviour towards information security policy compliance. Applying institutional theory, we posit that an employee's compliance behaviour with information security policy is positively influenced by regulative, normative and culture-cognitive forces in organisations.

1 Introduction

Numerous insider threats in recent years have challenged the capability of information security management in organisations, and raised critical questions about how organisations can effectively manage employees' behaviour to comply with IS security policies, standards and procedures. Development of such policies may be shaped by external guidance ranging from the broad and legal, such as the Sarbanes-Oxley Act of 2002 developed to address internal audit and corporate governance; to the directive and specific, such as the ISO/IEC 27000 series developed to strengthen information security management in organisations. These lead organisations to develop information security policies, provide information security training for employees, develop restricted information processing systems, implement virtual private networks (VPNs), and so forth. However, it is implementation more than development of procedures that matters. Employee behaviour in complying with IS security is critical, and yet organisations are finding that employees may choose to ignore internal audit and information security policies and procedures [12]

Much work has investigated computer abuse and misuse [30], employees' security behaviour [4, 14, 17], and information security policy compliance [14, 21, 29, 5]. Recent studies have developed a multi-level theoretical framework for understanding employees' attitudes toward compliance with information security policy. [22, 14] investigated motivational factors influencing employees' compliance behaviour based on deterrence theory and protection motivation theory. Bulgurcu et al. [5] identified

Hou Y., Gao P. and Heeks R..
The Influence of Institutional Forces on Employee Compliance with Information Security Policies.
DOI: 10.5220/0003587901320141
In *Proceedings of the 8th International Workshop on Security in Information Systems* (WOSIS-2011), pages 132-141
ISBN: 978-989-8425-61-4

factors influencing employee compliance with information security policy rooted in rational choice theory. "Insider" research has often adopted a criminological perspective and posited employees as information security policy (ISP) "offenders", while others have argued that employees may also be recognised as safeguards of ISP. Previous work addressed motivational (i.e. severity of security breaches, probability of security breaches), rational (i.e. benefit and cost of compliance/noncompliance) and environmental factors (i.e. facilitating conditions), but it hasn't been identified and recognised that employees' compliance with ISP is positively influenced by institutional factors, which an individual's compliance behaviour is significantly shaped by. In addition, previous researches have tested some components, but a systematic and integrated modelling is still missing.

In this research, we propose to apply institutional theory to understand individuals' security behaviour with compliance influenced by institutional factors. According to institutional theory, although individuals are self-interested, self-aware actors shaped by information processing and decision-making constraints, their behaviour is strongly shaped by environmental factors [11]. These environmental forces can be understood as regulative, normative and cultural-cognitive [24] (of which information security policy, standards and procedures would be one of the regulative forces). Bjorck [2] has taken this foundation to identify the gap between formal security structures and actual employees' security behaviour. He suggested institutional isomorphism can explain why information security policies and procedures come to be treated as 'paper tigers' in the organisations. In addition, why individuals differ in their actual security compliance behaviour is requires an understanding not only of regulative forces but also normative and culture-cognitive influences. However, he brought up the idea of applying institutional perspective to employees' security behaviour, he failed to give any evidence and rational explanation in information security policy context. Extending work after Bjorck [2], Hu et al. [16] studied the role of internal and external factors influencing the implementation of IS security practices and protocols, and how these factors affect managers and employees' cognition and shape their action on IS security. Similarly, although they found isomorphic forces such as, coercive and normative are important in influencing IS security implementation in the company, to our knowledge, the institutional forces are not recognised in information security policy context, especially cultural-cognitive forces. Therefore, understanding of what and how institutional factors influence employees actual behaviour toward compliance with ISP will be identified and analysed in this research. The rest of research in progress paper is organised as following. The second section will describe and discuss previous studies on employees' security behaviour, particularly compliance with information security policy. The third section will present a theoretical framework of institutional factors influencing employees' compliance. Potential research contribution will be discussed in the final section.

2 Previous Research on Security Behaviour and Information Security Policy Compliance

Due to the importance of behavioural aspects of IS security in organisations, research on organisational and behavioural information security has begun to emerge into IS security field. Organisational and behavioural knowledge of information security has been expanded since Dhillon and Backhouse [10] brought up their social-organisational perspective study on information system security. Issues related to IS security policy design [28], economics of information security [12], information security culture [9], information security behaviours [15], and information security management and governance [8] have highlighted a growing trend of research into IS security. In spite of these studies having extended our knowledge about different perspectives of IS security, the studies have tended to represent managers' perceptions about IS security while looking far less at employees: the actual participants who ultimately determine the success or failure of IS security governance, management, and policies.

To address the issue of employees' compliance with information security policy and procedures, employees' behaviour has been studied; representing the individual level of IS security. IS security behaviour studies primarily started with individuals' action, such as detecting and disciplining for computer abuse and misuse [30]. Employees' abuse and misuse of IS resources had been identified as a big issue in organisations [18]. In the early research on employees' behaviour on IS security, employees were assumed to be 'potential threats' to organisations [30, 31]. For instance, Straub and Nance [30] stated that internal computer abuses/misuse caused a huge loss in the United States and will continue in the future. Under this circumstance, they developed a process model for detecting, verifying, assessing and disciplining computer abuse, and suggested organisations should discipline staffs for serious computer abuse activities in order to deter similar behaviours [30]. The criminological theory was applied to understand prevention, deterrence and monitoring of employees' activities Hoffer and Straub 1989, [31]. But these have been criticised. For example, Willison [36] argued although criminological theories provide valuable insight into sanction on deterring future behaviours, they have limit on providing insight into criminal actual behaviour and how criminal behaviour is acting.

Besides computer abuse and misuse, in order to to encourage responsible security behaviour from employees, the attitude of viewing employees as 'offenders' has to be changed as employees can also help organisations safeguard information security. Several researchers have attempted to understand human behaviours affecting information security. Employee behaviour towards IS security is regarded as 'the person's actual response to a recommended behaviour and is the net effect of threat appraisal and coping appraisal' [37]. Vroom and von Solms [34] found auditing employees' behaviour is very difficult but that, through engaging organisational culture around security, there can be a positive influence on employees' behaviour. Dhillon and Mishra [20] suggested the theory of anomie is suitable for analysing the behavioural aspect of IS security governance through security culture, internal control assessment, security policy, individual values and security training.

In more recent research on this issue, social behaviour theories (e.g. the theory of planned behaviour, rational choice theory) have been applied to understand antecedents of security compliance behaviour through attitudes that shape intentions, while criminology theory fails to address on. Pahnila et al. [22] criticised prior information security policy compliance research which lack theory-grounded and empirical evidence and extended the knowledge of ISP compliance by proposing a multi-theory-based model to identify motivational factors that affect individuals' attitudes towards compliance, intention to comply and actual compliance behaviour. Herath and Rao [14] argued previous literature investigated motivational factors on overall context rather than the specific information security policy compliance context. They suggested employees' attitudes are influenced by coping with threats, and ISP compliance is affected by attitude and subjective norms.

In summary, then, to understand employees' information security behaviours, past researchers have identified and evaluated many important antecedents. Despite the criticisms, it seems that this research does include theoretical grounding and empirical testing of different contexts of information security policy compliance. This has included consideration of the effect of normative factors and perceived severity and coping appraisal. However, we still find that the external environment – particularly regulative and cultural influences on employees' behaviour toward information security policy – has not been particularly strongly analysed and tested in different contexts of IS security. Similarly, although normative beliefs have been evaluated in both policy and organisational contexts, they have not analysed in terms other than social subjective expectations. This paper undertakes these tasks in an attempt to provide an overall institutional model for helping understand employee behaviour toward information security compliance.

3 Theoretical Background and Research Model

As already noted, generally, research on IS security policy compliance has been evaluated from criminological and individual behavioural perspectives. Employees are treated as offenders and/or safeguards to information resources from these perspectives. Information security policies and procedures are seen as enacted to ensure employee obedience to certain rules, and information security awareness training and education is to make sure employees understand their responsibilities to information assets in the organisations. To summarise the literature review, information security behaviour researches have borrowed criminology theory to deter criminal behaviour on sanction. The sociology theories are to understand individuals' behaviour on IS security, and help to predict and explain individuals' behavioural preferences. Similarly, issues concerned about employees' compliance drew on social behaviour theory to analyse employees' attitude and intention to comply with information security policy. However, to our knowledge, previous research are lack to address the external environment influencing on employees' compliance behaviour towards ISP, particularly regulative and cultural effects. In order to fill in the gaps, this study applies institutional theory to help explain how behaviours are influenced by institutional effects from national, organisational and individual level. In this research, we adopt three categories of forces from institutional theory – regulative, normative and cultural-cognitive – as the antecedents of employee behaviour vis-a-vis ISP compliance. A theoretical model consisted of institutional factors explains employees' behaviour compliance with ISPs. Our research model provide a valuable theoretical contribution to the knowledge of behavioural and organisational issues on information security. This is the first study applying institutional theory to understand employees' compliance behaviour toward information security policy in organisations.

3.1 Individual Compliance Behaviour and Institutions

An individual's behaviour usually refers to that individual's reaction to social norms and regulations within a social context or environment. Compliance is the conforming responding to requests and rules. Compliance in relation to IS security involves an individual abiding by the IS security policies and procedures in an organisational context, while non-compliance behaviour is vice versa. Thus, employees' compliance behaviour towards information security policies or procedures should be conceptualised as individual behaviour influenced by external forces in the organisations. Through the literature, employee compliance behaviour can be influenced by various institutional mechanisms including legal instruments, economic sanctions and normative beliefs [22, 14, 5]. Institutional theory is widely used in politics, economics and social science in studying individual or organisational behaviour. For instance, Axelrod [1] studied how individuals pursue self-interest and found out individuals' behaviours are significantly influenced by institutional regulation. Blackstock et al. [3] explored institutional mechanisms influencing farmers behaviour in order to reduce water pollution diffusion and found out social and cultural influences both exist in control over mitigation water pollution.

According to Scott [24], institutions 'consist of cognitive, normative, and regulative structures and activities that provide stability and meaning to social behaviour'. We can now look at these three institutional forces in a little more detail. Regulative forces in organisations refers to 'institutions that constrain and regularise behaviour' [24]. Normally regulatory processes begin with rule-setting and then include monitoring and sanctioning activities. This emphasises that the behaviours of individuals 'are ruled' by written or unwritten codes of conducts. From the institutional view, IS security is supported by surveillance and sanctioning power, and individuals' compliance behaviour is affected by 'cost-benefit calculations' to regulations [13]. Normative force emphasises prescriptive, evaluative, and obligatory aspects in society [23]. There are two elements in normative systems: values and norms. Values are conceived as preferences which can be compared and assessed, while norms refer to 'how things should be done' [24] and objectives of the systems. In institutional theory, a normative system not only defines goal and objectives, but also designs appropriate ways to achieve it [24]. Normative institutions are concerned with how values and norms structure individual choice. The cultural-cognitive perspective relates to knowledge and meaning. Scott [23], for example, states that 'cognitive elements constitute the nature of reality and the frame through which meaning is made'. Individual behaviour is viewed as reflecting external social constitution rather than internal intentions [23]. According to cognitive theorists, compliance occurs because 'other types of behaviour are inconceivable' and it takes for granted as it is the way to do things right [24].

3.2 Institutional Theory and Application to Information Security Behaviour

Institutional theory focuses on how external structures interact within organisations. It proposes how social behaviour (choice) is influenced, mediated and guided by the institutional environment [11]. Institutional theory goes through a history from 'old institutional theory' [25, 26] to 'new institutional theory' [11, 19, 23]. Institutional theory was largely applied in organisational studies and it has turned its attention to information systems studies over the past two decades. For example, Butler [6] used institutional theory to explain the behaviour of social actors in development of a web-based information system. Teo et al. [32] conducted a survey based study to test three types of institutional forces influencing adoption of inter-organisational system. Chiasson and Davidson [7] examined IS research using institutional theory from MIS Quarterly and Information Systems Research to demonstrate the importance of industry influences on IS activities. In recent years, institutional theory has thus become one of the major theoretical frameworks for understanding IS innovation.

Only two research papers were located using institutional theory to illustrate the socio-organisational factors important in information security research. The first information security study employing institutional theory is Bjorck [2] who used neo-institutional theory to explain the difference between formal security structure and actual security behaviour. He created a new perspective on viewing information security behaviour. Hu et al. [16] fully adopted Scott's perspective of organisational behaviour and used institutional theory as a theoretical framework to analyse external and internal factors influencing organisational behaviours and organisational actor behaviours. Drawing from Bjorck [2] and Hu et al. [16], the research aims to use institutional theory to develop an institutional-organisational framework to analyse in detail how institutional and organisational factor influence information security management strategy rather than employees' compliance behaviour towards ISP. In addition, Bjorck's work is lack of empirical evidence and explaination of how employees' compliance with ISP is influenced by institutional factors. Both research have not evaluated institutional factors in information security policy context through national, organisational, individual level analysis.

3.3 Research Model

Based on institutional theory, we propose a framework for understanding what factors influence employees' behaviours and result in their compliance with IS security policies (Figure 1). Institutional theory suggests that regulative, cultural-cognitive and normative forces can shape social behaviour in organisations [23]. In our theoretical model, it posits that the institutional environment (i.e. national, organisational and individual level) provides regulative, normative and cultural-cognitive influences on employees' security behaviour in organisations. In the previous section, we showed briefly how regulative, normative and cultural-cognitive influences shape behaviour, indicating that employees are situated within a complex environment, which from national, organisational and individual levels. In this section, we will identify three levels institutional forces factors, and extend literature behaviour-influencing factors based on institutional theory, by creating a systematic model from that past work.

According to Scott [24] three institutional forces characteristics, at the national level, the behaviour receives impact from legal, regulation and culture norms, such as national policies, government control, law regulations and national culture (Table 1). At the organisational level, organisational culture, roles, procedures, regulations, and technical capability (e.g. security knowledge), which may affect employees' compliance behaviour (Table 2). At the individual level, the compliance behaviour is affected by employees' commitment and convention, colleague and IT professional impact, and individual awareness (Table 3). As regards to institutional forces, regulative forces come from national legal instruments, and from policies and detection and assessment systems within the organisation. Herath and Rao [14] claimed there is a significant effect on policy compliance intention from the certainty of detection, but no sanctioning effect on employees' intention to comply with ISP. We posit government control, national law, organisational policies and rules, and employee assessment will affect employees' behaviour toward ISP compliance. Normative forces also play an important role in shaping individuals' behaviour. Pahnila et al. [22] investigated 245 employees' ISP compliance and found out normative beliefs (i.e. values from top managers, supervisors, colleagues and IS security professional) are important in strengthening employees' intention to comply with ISP. We posit norms such as industry standards, international standards, especially information security procedures have an effect on employees' compliance with ISP. Recent studies on cultural aspects suggests organisational culture impacts information security behaviour [33] and that, for example, a security awareness culture can reduce employees misbehaviour [9]. In addition, policy compliance can be also seen as a type of cultural-cognitive behaviour in which routines may seen as taken for granted rather than obligations. Thus, in our study, employees' actual security behaviour are determined by regulative, normative and cultural-cognitive factors within organisations.

In order to evaluate our research model, a in-depth case study will be studied. However, this is a research-in-progress short paper, the potential investigation is still in progress. In this paper, we take an example instead of real case study to present a useful explanation for better understanding the socio-organisational issues in a company's employees' compliance behaviours with information security policies. In an organisation, employees' security behaviour are restricted by organisational policies, rules, procedures and regulations. These organisational policies and procedures are enacted according to national policies or even politics, and international standards. Comparing to regulative and normative forces, the culture force focuses on 'soft' and long-term impact on employees' behaviour. For instance, culture forces come from three resources: national culture, organisational culture and individual awareness, and individuals' self-awareness characteristic influence the behaviour of security compliance. In summary, employees' compliance behaviour is directly affected by regulative, normative and culture-cognitive forces in three different levels.

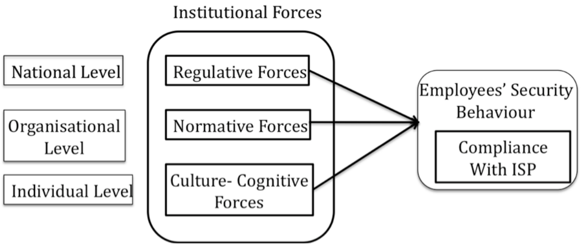

Fig. 1. Theoretical research framework.

Table 1. National Level Institutional Forces.

Institutional Forces	Features
Regulative Forces	National politics and policies, Government Control
Normative Forces	International Standards, Best Practise, International Industry Standards,
Culture-Cognitive Forces	National Culture

Table 2. Organisational Level Institutional Forces.

Institutional Forces	Features
Regulative Forces	Organisational Policies, standards, rules, regulations,
Normative Forces	Organisational security procedures, certificates, rights, responsibilities, knowledge
Culture-Cognitive Forces	Organisational Culture, organisational awareness

Table 3. Individual Level Institutional Forces.

Institutional Forces	Features
Regulative Forces	self-constrain,
Normative Forces	colleagues and expertise's impact, individual convention
Culture-Cognitive Forces	individual awareness

4 Potential Contribution and Future Research

In this paper, we provided a three level institutional forces model rooted in Scott’s institutional theory to explain employees’ security compliance behaviour. We analysed past researches and proposed a research design to fill in the gap: how regulative, normative and culture-cognitive forces influences employees’ security compliance behaviour. We will further specify a set of specific factors that affect employees’ ISP compliance behaviours and justify the effects of each factor. We also tend to empirically test our theoretical model with single deep qualitative case study in the organisation. The abductive approach will apply in this research for analysing collected data. Previous literature and institutional theory will be used as ‘sensitising theory’ to guide the research. The main data collection method will be semi-structured interviews. The aim is to collect data on institutional forces influencing ISP compliance at national, organisational and individual level. The interviews will be conducted among the Board, Chief Security Officer, department managers, project managers, employees, and the policy makers. The interviewees will widely cover the topics of enacting, implementing and deployment ISP and compliance behaviour in the company and relative national government departments. Comparing to previous quantitative survey investigations, our qualitative case study provide valuable comprehensive data highlighting the social, cultural and organisational issues directly from people.

References

1. Axelrod, R., 1984. The Evolution of Cooperation. Basic Books, New York.
2. Bjorck, F., 2004. Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations. In Proceedings of the HICSS 04 Working Conference on Information Systems Security Management, 186-190.
3. Blackstock, K. L., Ingram, J., Burton, R., Brown, K. M. and Slee, B., 2010. Understanding and Influencing Behaviour Change by Farmers to Improve Water Quality. Science of the Total Environment, 408 (23), 5631-5638.
4. Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W., 2009. If Someone Is Watching, I'll Do What I'm Asked: Mandatories, Control, and Information Security. European Journal of Information Systems, 18 (2), 151-164.
5. Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34 (3), 523-548.
6. Butler, T., 2003. An Institutional Perspective on Developing and Implement Intranet - and Internet -Based Information Systems. Information Systems Journal, 13 (3), 209-231.
7. Chiasson, M. W. and Davidson, E., 2005. Taking Industry Seriously in Information System Research. MIS Quarterly, 29 (4), 591-605.
8. Da Veiga, A. and Eloff, J. H. P., 2007. An Information Security Governance Framework. Information Systems Management, 24 (4), 361-372.
9. Da Veiga, A. and Eloff, J. H. P., 2010. A Framework and Assessment Instrument for Information Security Culture. Computer & Security, 29 (1), 196-207.
10. Dhillon, G. and Backhouse, J., 2001. Current Directions in Information Security Research: Toward Socio-Organisational Perspectives. Information Systems Journal, 11 (2), 127-153.
11. DiMaggio, P. J. and Powell, W., 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organisational Fields. American Sociological Review, 48 (3), 147-160.
12. Gordon, L. A., 2006. Economics Aspects of Information Security: An Emerging Field of Research. Information Systems Frontier, 8 (5), 335-337.
13. Hechter, M., Opp, K. D. and Wippler, R., 1990. Social Institutions: Their Emergence, Maintenance and Effects. eds. Aldine de Gruyter, New York and Berlin.
14. Herath, T. and Rao, H. R., 2009a. Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems, 18 (2), 106-125.
15. Herath, T. and Rao, H. R., 2009b. Encouraging Information Security Behaviours in Organisations: Role of Penalties, Pressures and Perceived Effectiveness. Decision Support Systems, 47 (2), 154-165.
16. Hu, Q., Hart, P. and Cooke, D., 2007. The Role of External and Internal Influences on Information System Security- A Neo-Institutional Perspective. Journal of Strategic Information System, 16 (2), 153-172.
17. Johnston, A. C. and Warkentin, M., 2010. Fear Appeals and Information Security

Behaviours: An Empricial Study. MIS Quarterly, 34 (3), 549-566.

18. Loch, K., Carr, H., and Warkentin, M., 1992. Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly, 17 (2), 173-186.
19. Meyer, J. W. and Rowan, B., 1977. Institutionalise Organisations: Formal Structure as Myth and Ceremony. American Journal of Sociology, 83 (2), 340-363.
20. Mishra, S. and Dhillon, G., 2006. Information Systems Security Governance Research: A Behavioural Perspective. 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, New York, USA.
21. Myyry, L., 2009. What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study. European Journal of Information Systems, 18 (2), 126-139.
22. Pahnila, S., Siponen, M. and Mahmood, A., 2007. Employees' Behaviour Toward IS Security Policy Compliance. In proceedings of the HICSS 07 Working Conference on Information Systems Security, Los Alamitors, CA: IEEE Computer Society Press, 155-166.
23. Scott, W. R., 1995. Institutions and Organisations. Thousand Oaks, California.
24. Scott, W. R., 2001. Institutions and Organisations. 2nd edition, Thousand Oaks, California.
25. Selznick, P., 1949. TV and the Grass Roots. Berkerley, University of California.
26. Selznick, P., 1957. Leadership in Administration: A Sociological Interpretation. Evanston III, Peterson.
27. Siponen, M. T., 2000. A Conceptual Foundation for Organisational Information Security Awareness. Information Management & Computer Security, 8 (1), 31-41.
28. Siponen, M. T. and Iivari, J., 2006. Six Design Theories for IS Security Policies and Guidelines. Journal of the Association for Information Systems, 7 (7), 445-472.
29. Siponen, M. T. and Vance, A., 2010. Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, 34 (3), 487-502.
30. Straub, D. W., 1990. Effective IS Security: An Empirical Study. Information Systems Research, 1 (3), 255-276.
31. Straub, D. W. and Welke, R. J., 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 22 (4), 441-469.
32. Teo, H. H., Wei, K. K. and Benbasat, I., 2003. Predicting Intention to Adopt Interorganisational Linkages: An Institutional Perspective. MIS Quarterly, 27 (1), 19-49.
33. Van Niekerk, J. F. and Von Solms, R., 2010. Information Security Culture: A Management Perspective. Computer & Security, 29 (4), 476-486.
34. Vroom, C. and von Solms, R., 2004. Towards Information Security Behavioural Compliance. Computer & Security, 23 (3), 191-198.
35. Warkentin, M. and Willison, R., 2009. Behavioural and Policy Issues in Information Systems Security: the Insider Threat. European Journal of Information Systems, 18 (2), 101-105.
36. Willison, R., 2006. Understanding the Perpetration of Employee Computer Crime in Organisational Context. Information and Organisations, 16 (4), 304-324.
37. Woon, I. M. Y., Tan, G. W. and Low, R. T., 2005. A Protection Motivation Theory Approach to Home Wireless Security. In Proceeding of the Twenty-Sixth International Conference on Information Systems, 367-380.