RELATIONSHIP BETWEEN INFORMATION SECURITY AWARENESS AND INFORMATION SECURITY THREAT

WILLIAMS SOLOMON ADEDAYO
STUDENT
SCHOOL OF COMPUTING
UNIVERSITI UTARA MALAYSIA
MALAYSIA

AKANMU SEMIU AYOBAMI
RESEARCH SCHOLAR
SCHOOL OF COMPUTING
UNIVERSITI UTARA MALAYSIA
MALAYSIA

ABSTRACT

Information security threat has been reported to be on the increase among users of internet technologies, especially the academic communities, comprising the students, lecturers and tutors. In attending to this situation, past studies have either conceptually discussed or empirically studied some related factors to information security threat generally, with few (if at all any) studied information security awareness' relationship within the conceptual framework of community training, vulnerability to threat, perceived threat severity and compliance to security policies with information security threat. And none has studied this among the Universiti Utara Malaysia community. This paper studies these factors in view of the relationship between information security awareness and information security threat among the Universiti Utara Malaysia students' community. This study uses Quantitative method, with Pearson correlation as the statistical tool. The findings of this study showed that community training; vulnerability to threat, perceived threat severity and compliance to security policies within the concept of information security awareness is positively related to information security threats.

JEL CODE
M15

KEYWORDS
community training, information awareness, information security threats, perceived threat severity, vulnerability to threat.

INTRODUCTION

The development that takes place in internet and computer networking technology has consequently led to security challenges as evident in the increase of information threats. This development has undoubtedly necessitated new security measure and policies to reduce the intensity of the threat and the challenges being encountered from the emergence of the new technology (Alshboul 2010).

It is noticed that new technology is very easy to adopt and be adapted with, but most institutions do forget to put a security measure in place in order to safeguard the organization information from being tampered with. Information Integrity is essential, and this is about trustworthiness, origin, completeness and correction of information, with due obstruction of unauthorized modification of information (Al-Awadi et al., 2007; Baker & Wallance, 2007). The integrity of information security in this context is not concerned about organizations only, but also expands to the integrity of the source of information and the users who are in charge of the organizations' information systems. Most importantly, it is observed that threats of information leakage are experienced more when the students share the data of the organization and is compromised by an intruder's intervention. Many encountered problems of threats and viruses in Universiti Utara Malaysia (UUM) are sometimes as a result of negligence on the part of the staff or the administrators that are in charge of the organization information and data mart.

Mikko (2000) disclosed that when an unauthorized personality or user has the access to information system and discloses the content of the confidential document or information, it has a bad effect in the security and privacy of the community. Therefore, the UUM management has a role to play in the security of information of the UUM community, and the users should be fully aware of such incoming threat so as to safeguard their respective information from intruder (Sraub and Welke, 1998). In the same vein, Siponen (2000) and Benzel et al., (2012) affirmed that the organization top manager, meddle manager and even the workers do ignore the issues bothered on security, and the outcome of this neglect in any organization as seen in UUM system are worst damaged more than the expectation.

REVIEW OF LITERATURE

THE RELATIONSHIP BETWWEN COMMUNITY TRAINING AND INFORMATION SECURITY THREATS

Dutta & Mcrohan (2002) suggested that establishing the concept of network security is important. Therefore, users of the information system must be actively engaged in education and training that will enhance security awareness. They stated that the education should mainly aim at how the security policy safeguards the organization information from the intruders. He explained that the organization should be conducting training that will inform the community of specific actions that are necessary to be put in place to protect them against the security threats or violence. Training should involve specific technical equipment that will mitigate information security threat on information system.

Dhillon (2000) stated that the organization should engage in the basic education and training program to achieve expected result from the implementation of information security policy. Lampson (2002)'s view is that the negligent of the employees on duty could consequently give the hackers a full privilege to perpetrate their illicit act on the organization system. More carelessness in log off while on break or closing period recording passwords on sticky note on the computer system or sharing the confidential document with unauthorized person. The expected effort is to get the community trained on basic thing they have to know. Giving a basic training and making them to know the consequence of security threat, this could make them to be fully aware and be conscious of hackers and intruders.

THE RELATIONSHIP BETWEEN VULNERABILITY TO THREATS AND INFORMATION SECURITY THREATS

Claar (2011) and Brahim and Zhao (2009) argued that vulnerability of the user or individual judgment about the danger of his or her information is inside the computer system. Vulnerability to threats is the weakness of information and information system. This can consequently lead to attack, modification and destruction. The new threat occurs when an organization relies on it. Johnston (2010) expanded on threat as a symbol that indicates the incoming dangers. Kumar & Subramanian (2008) argued it to be a condition of vulnerability that could result to insecurity of an organization security.

Alshboul (2010) and Humaidi & Balakrishnan (2004) examined the information system security measures: protecting organization asset from malicious attack. The research constructed a method that gave the definition of information security level in organization. Given the definition of information security this level affirms with measuring security layers which are network security, physical security and personal security in the companies. The study tried to find the correlation between the company's assets, security vulnerability, security attack and determining the security level, so as to protect the integrity, availability and also the confidentiality of the organization's asset.

THE RELATIONSHIP BETWEEN PERCEIVED THREATS SEVERITY AND INFORMATION SECURITY THREATS

In the words of Joo et al. (2011), the determinants of information security that are affecting the adoption of web-based information systems are analyzed. For this reason, a theoretical model was designed to examine the relationship between organization factors deterrent efforts and severity; preventive effort and individual factor of information security threat; security awareness and intention to actively use the web-based IIS. The outcome of the analysis stated that deterrent severity is not related with proactive used intention of ISS while the preventive effort has a relationship with proactive use of intention of IIS.

Stephanou et al (2008) and Casmir (2005) examined the insider misuse of information system resource. According to him, the information system misuse has been posing a great challenge to organizations. Their aim was to present the extended deterrence theory model that consists of study from criminology, information system and psychology. The model shows that the awareness of security countermeasures directly influences the perceived severity and certainty of punishment that come with information systems misuse which can make the information system to reduce misuse intention. The outcome of the study suggested that three practices deter information misuse, training and awareness program; user awareness of security policies, security education and computer monitoring. The outcome also suggested that the perceived severity of sanction may be more efficient in bringing down the information security misused more than certain sanctions.

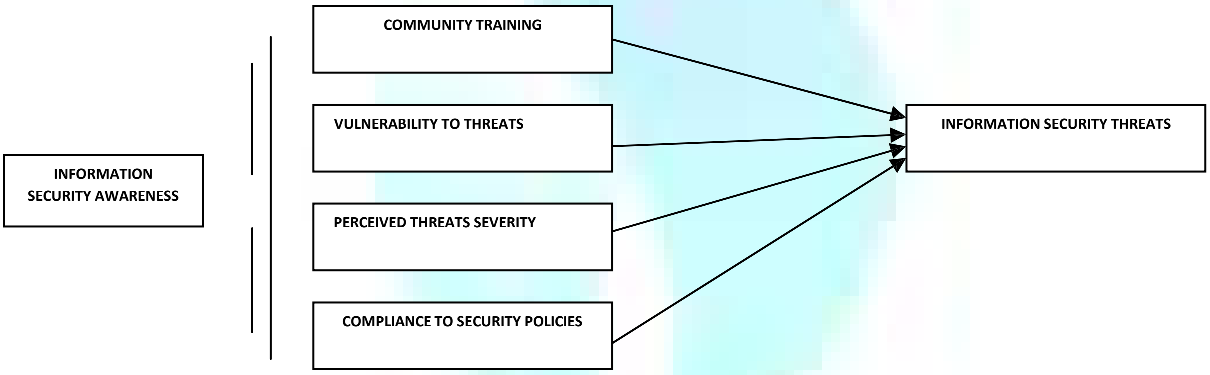
THE RELATIONSHIP BETWEEN COMPLIANCE TO SECURITY POLICIES AND INFORMATION SECURITY THREATS

Siponen et al (2007) studied employees' failure in compliance with the information system security. To address the compliance of the employees, he integrated habit which is the form of the behaviors. The empirical test showed that the habitual information system security with compliance will adaptively persuade the process. He also found out that nearly all the components are positively related to employees' intention to agree with information system security policies. The result thus shows that there is a relationship between the two. Significantly, it highlights the reason for addressing employee's past and automatic behavior so that there will be an improvement in compliance.

Herath & Rao's (2009) study on a theoretical contract model and information security model. This model was tested to evaluate and determine the relationship between penalties, pressure, the perceived and effectiveness of employees' responses and the understanding of employees' compliances to information security policies. The result of the examination shows that security behavior can act both as intrinsic and extrinsic motivators. The pressure applies by subjective tradition and friend behaviors influence employee's information security habit. The intrinsic motivation of workers perceived effectiveness of their respective action is discovered to have a crucial role to play in security policy and compliance intention. The findings showed that the penalties and the assurance of detection were found to have a significant role while the severity of punishment has a negative effect on a security habit of compliance intention. The result showed that the severe punishment is negatively related to compliance of employees in any companies' information security. Because of this, the adoption of awareness could be better applied than the severity punishment.

THE RESEARCH MODEL

FIGURE 1: BELOW GIVES THE CONCEPTUAL RESEARCH MODEL OF THIS STUDY.


INFORMATION SECURITY AWARENESS
COMMUNITY TRAINING
VULNERABILITY TO THREATS
PERCEIVED THREATS SEVERITY
COMPLIANCE TO SECURITY POLICIES
INFORMATION SECURITY THREATS

IMPORTANCE OF THE STUDY

This study derives its niche from the limitations of previous studies as stated above, and these consequently form the base of this particular research. This study critically and empirically looks at the relationship between information security awareness and the information security threat. The contents of the awareness will be used and evaluated are the training, vulnerability, perceived severity of the security threat and compliance with security policies.

This study's contribution and significances are: (1) the conceptualization of information security awareness using training, vulnerabilities, perceived severity of security threat and compliance with security policies, then (2) the empirical study of their relationship and its contextual application to the Universiti Utara Malaysia's community.

STATEMENT OF THE PROBLEM

The limitation from previous studies and the recommendation by Herath & Rao's (2009) on the need to re-conceptualized information security awareness necessitate this study. Lampson (2002) argued that organization will continuously be facing the issue of threat and insecurity due to the high cost maintenance of security facilities, and its sustenance. It is on this premise that this study want to answer a central question that: What is the relationship between information security awareness and information security threats in University Utara Malaysia's community, conceptualizing information security awareness using community training, vulnerability to threat, perceived threat severity and compliance to security policies?

OBJECTIVES

The objectives of this study are to study the relationship between:

i. Community training and information security threat,
ii. Vulnerability to threat and information security threat,
iii. Perceived threats severity and information security threat; and
iv. Compliance to security policies and information security threats.

HYPOTHESES

The hypotheses to be tested by this study are four; these are:

H_1 Community training has a relationship with information security threats
H_2 Vulnerability to threats has a relationship with information security threats.

H_3 Perceived threats severity has a relationship with Information security threats.

H_4 Compliance to security policies has a relationship with information security threats.

RESEARCH METHODOLOGY

Research methodology involves four different phases: the definition of the problem, data collection, data analysis, and reporting (Sekaran, 2006). These are designed and tailored to precisely answer the research questions, test the hypotheses and achieve the research objectives. The data collection being an important stage of the research process highlights the appropriate selective mode showing the correct use of instrument. This study utilizes an adapted self administered Questionnaire as an instrument of data collection.

The data analysis is be done with the appropriate statistical tools in SPSS, and with the descriptive analysis and correlation to answer the earlier posed research questions and achieve the research objectives. The last stage of the research is the Reporting, it constitutes of the research findings and analysis, and the interpretation of the analysis, conclusion of the research. It is important that at the study's conclusion, the stated objectives and elicited questions of this study would have been appropriately answered.

POPULATION AND SAMPLING

Population in the research context is understood as the total number of the elements in a study, and the sampling is the process of appropriately deciding on the representative selected group from the bigger population (Babbie, 2010). Kumar (2011) argued that random sampling as the appropriate form of probability sampling; that is for a study that has access to a demarcated and accessible study population. Babbie (2010) affirmed the correctness of random sampling and suggested different ways on how to go about selecting respondent randomly.

The population used in this study is graduate students of school computing and multimedia comprising of both the Master students and PhD students which amount to 440. The population comprises of UUM's post graduate students with regular use of internet and thus has full knowledge of what information security is all about. According to Krejcie and Morgan (1970), a population range between 440 will have a sample size of 205. To ensure the accuracy of this study's findings, the researcher makes use of 205 as the sample size, but a response rate of 73% was made, hence made the number of the respondents to be 150.

CONSTRUCT VALIDITY

Construct validity is by testing how reliable is the instrument items under each variable constructed of the questionnaire. This is done with the use SPSS reliability test. The Cronbach's Alpha level is then interpreted to determine the reliability of the item of each variable construct.

RESULTS AND DISCUSSION

RESULTS

The results of the statistical analysis are presented in this section. The results of the reliability tests, hypothesis 1, 2, 3 and 4 are given in tables 1, 2, 3 and 4 respectively.

RELIABILITY TEST

The reliability test for this study is done using construct reliability after the original data of the study is gathered from the respondents. The result is then compared with that of the pilot study using a uniform scale validation so as to examine the consistency of the study instrument. Table 1 presents the reliability testing with the pilot testing.

TABLE 1. RELIABILITY TEST

No	Variable	No. of Item	Pilot Test	Main Test
1	Community Training	5	0.798	0.781
2	Vulnerability to Threats	5	0.732	0.703
3	Perceive Threat Severity	5	0.745	0.702
4	Compliance to Security Policies	5	0.738	0.703

TABLE 2: RESULT FOR HYPOTHESIS 1

INFORMATION SECURITY THREATS		
Community training	Pearson Correlation Sig. (2-tailed) N	.791** .000 150

**Correlation is significant at the 0.01 level (2-tailed).

TABLE 3: CORRELATION RESULT FOR HYPOTHESIS 2

INFORMATION SECURITY THREATS		
Vulnerability to threats	Pearson Correlation	793**
	Sig. (2-tailed)	.000
	N	150

**Correlation is significant at the 0.01 level (2-tailed).

TABLE 4: CORRELATION RESULT FOR HYPOTHESIS 3

INFORMATION SECURITY THREATS		
Perceived threats severity	Pearson Correlation	741**
	Sig. (2-tailed)	.000
	N	150

**Correlation is significant at the 0.01 level (2-tailed).

TABLE 5: CORRELATION RESULT FOR HYPOTHESIS 4

INFORMATION SECURITY THREATS		
Compliance to security policies	Pearson Correlation	751**
	Sig. (2-tailed)	.000
	N	150

**Correlation is significant at the 0.01 level (2-tailed).

DISCUSSION

From the descriptive analysis of this study, the respondents' demographics were not essentially captured because they are not of importance in studying the relationship between information security awareness and information security threats. The part attended to was the gender distribution, and this study recorded more male respondents than the female. However, the gender frequency is of no specific interest, therefore, the descriptive statistics has no importance.

Specifically, they are postgraduate students, thus conforms with the need to make the enquiry from a set of respondents that can objectively and accurately respond to the set of items in the questionnaire. This will ensure precise answers to the research questions expected to be answered in testing the hypotheses of this study.

COMMUNITY TRAINING HAS RELATIONSHIP WITH INFORMATION SECURITY THREATS

This study has inferred from its findings that community training relationship with information security threats. Siponen et al (2007) findings supported the empirical findings of this study, stating that awareness through training has a relationship with information security threat. The contents of the awareness was explicitly said to be training and compliance with security policies.

VULNERABILITY TO THREATS HAS RELATIONSHIP WITH INFORMATION SECURITY THREATS

In support of the finding of this study that vulnerability to threat is related to information security threat, Joo et al (2011) reported that there is an association between the company's assets, security vulnerability, security attack and determining the security level, in protecting the integrity, availability and also the confidentiality of the organization's asset. The study also agreed that vulnerability to threat endangers the company's confidentiality, hence increases information security threats.

PERCEIVED THREATS SEVERITY HAS RELATIONSHIP WITH INFORMATION SECURITY THREATS

This study, from the empirical findings found that perceived threat severity has a relationship with information security threats. From past related works, Joo et al (2011) in their study reported that deterrent severity is not related with the proactive used intention of Information systems while the preventive effort influences the proactive use of Information systems security. Siponen et al (2007) from their findings submitted that the awareness of security countermeasures has a relationship with the perceived severity and certainty of punishment that comes with information systems. Also, Herath & Rao (2009) found that severity of punishment have a negative relationship on a security habit of comply intention. It is further stated that severe punishment influences the employees' compliance in any companies to information security. Thus, submitted that the adoption of awareness could be better applied than the severity punishment.

COMPLIANCE TO SECURITY POLICIES HAS A RELATIONSHIP ON INFORMATION SECURITY THREATS

The result of this study is that compliance to security policies has impact on information security threats. Notably, past studies have not singly pointed to compliance to securiy policies as a factor leading to information security threats. Like Siponen (2000), Herath & Rao (2009) and SD'Arcy et al. (2009), perceived severity has been studied to have a direct linkage with compliance to security policies, subsequently affecting information security threat. This study, among other few ones studied the impact of compliance to security policies directly on information security threat, and also found that they are related with compliance to security policies having impact on information security threats.

FINDINGS

RESEARCH HYPOTHESES' TESTING

As earlier stated, this study analyses and test the study's hypothesis using SPSS. Pearson product-moment correlation was used to test the research hypotheses as related in the relationship between the independent and dependent variables. This is done after due data screening and cleaning. The inferential analysis is to study the relationship between the independent variables and the dependent variable. In doing this, Correlation as a statistical tool was used (Sekaran, 2006; Hair et al, 2008; and Pallant 2011).

H_1 Community training has a relationship with information security threats

The hypothesis of the relationship of community training on information security threats as elicited in this study uses Pearson product-moment correlation for its testing. A high directional (positive) correlation between community training and information security threat was found, this equation explains the result of the correlation [r—0.791, n-150, p<.05]. It is thus shown that the 79% variance in community training could be explained by 79% changes in information security threats variable. With the significance less than 0.05, it shows that the tested hypothesis is accepted. The result presented in Table 4.3 is therefore achieves the first research objective.

H_2 Vulnerability to threats has a relationship with information security threats.

The second hypothesis of this study is also tested with Pearson product-moment correlation, confirming the hypothesis of the relationship of vulnerability to threats variable on information security threat. The correlation result as shown in Table 4.4 shows a high positive relationship between vulnerability to threat and information security threat, [r—0.793, n-150, p<.05]. This can be interpreted that the 79% variance in vulnerability to threat is associated to 79% variances in the information security variable. This achieves the second research objective, and the hypothesis is accepted.

H_3 Perceived threats severity has a relationship with Information security threats.

The third hypothesis of this study is equally tested with Pearson product-moment correlation, and the result of the correlation is presented in Table 4.5. The result states that there is a correlation coefficient between perceived threats severity as a variable, and speaking anxiety. The result is further explained with the following correlation equation [r—0.741, n-150, p<0.05]. It shows that 74% variances in perceived threats severity is explainable by 74% variances in its relations with Information security threats. This answers the third research question, and shows the research objective is achieved.

H_4 Compliance to security policies has a relationship with information security threats.

The fourth hypothesis of this study is tested with Pearson product-moment correlation also, and the result of the correlation is presented in Table 4.6, showing that there is a correlation coefficient between compliance to security policies and information security threats. This result can be further explained using the following correlation equation [r—0.751, n-150, p<0.05]. It is that 75% variances in compliance to security policies explain 75% variances in the relations with Information security threats variable. This result answers the last question of the study that: What is the impact of compliance to security policies on information security threats?, hence achieves the fourth research objective.

RECOMENDATIONS

RECOMMENDATIONS FOR FUTURE STUDY

Continuous nature of research is an unavoidable happening, as one research's conclusion opens the necessity for another research. From the conclusion of this study, the future studies recommended are:

1. Using other SPSS statistical tool like Regression to further examine the effect of dependent variables on the independent variables
2. Employment of more statistical analysis tool like Structural Equation Modelling to strengthen the inferential analysis of this study
3. Employment of mixed method research, by consolidating the research findings with Qualitative methods to examine further studies.

CONCLUSION

From the literature review, the data analysis, results and the research findings agreed with the hypotheses tested by this study. This study objectively established the facts that each of the independent variables of this study: community training, vulnerability to threats, perceived threat severity, and compliance to security policies is positively related to the dependent variable; Information security threat.

This study has further added to the weight of previous studies on the relationship of community training, vulnerability to threats, perceived threat severity, and compliance to security policies on information security threat with due empirical findings. This study has further strengthened past related works that submitted similar findings as regards information security threat reduction, and becomes important for policy makers, information security experts and information technology users in fostering information security. Conclusively, this study delivers an empirical result that community training, vulnerability to threats, perceived threat severity and compliance to security policies summing up to information security awareness have impact on information security threat among the Univerisiti Utara Malaysia's students community.

REFERENCES

1. Al-Awadi, M., & Renaud, K. (2007), "Success factors in information security implementation in organizations," Paper presented at International conference on e-society.
2. Alshboul, A. (2010), "Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks," Communications of the IBIMA.
3. Babbie, E. (2010), "The Practice of Social Research", 12th Edition. Wadsworth Cengage Learning, USA.
4. Baker, W. H., & Wallace, L. (2007), "Is information security under control?: Investigating quality in information security management. *Security & Privacy," IEEE*, *5*(1), 36-44.
5. Benzel, T. V., Irvine, C. E., Levin, T. E., Bhaskare, G., Nguyen, T. D., & Clark, P. C. (2012), " Design principles for security," IEEE Transaction on Security, 29-38
6. Brahim, A., & Zhao, l. (2009),"Supporting the osgi service platform with mobility and service distribution in ubiquitous home environments", *The Computer Journal*, 52(2), pp 210-239.
7. Casmir, R. (2005): "Dynamic and adaptive information security awareness (DAISA) approach", Dissertation, University of Stockholm.
8. Claar, C. L. (2011): "The Adoption of Computer Security: An Analysis of Home Personal Computer User Behavior Using the Health Belief Model", Dissertation, Utah State University.
9. Dhillon, G., & Backhouse, J. (2000), "Technical opinion: Information system security Management in the new millennium", *Communications of the ACM*, Vol. *43*(7), pp 125-128.
10. Dutta, A., & McCrohan, K. (2002), "Management's role in information security in a Cyber Economy," California *Management Review*, Vol. *45*(1), pp 67-87.
11. Gaston, S.J. (1996), "Information security: security strategy for successful management". CICA Publishing, Toronto.
12. Hair, J.F., Black, W., Babin, B., & Anderson, R. (2009), "Multivariate Data Analysis". Prentice Hall, UK.
13. Herath, T., & Rao, H. R. (2009), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", Decision Support Systems, Vol. 47(2), pp 154-165.
14. Humaidi, N., & Balakrishnan, V. (2004), "The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework", Communications of the ACM, Vol. 40(3), pp 57-59
15. Johnston, A. C., & Warkentin, M. (2010), "Fear appeals and information security Behaviors: an Empirical study. *Mis Quarterly*, Vol. *34*(3), 549.
16. Joo, J., Kim, M. J., Normatov, I., & Kim, L. (2011), "Determinants of Information Security Affecting Adoption of Web-based Integrated Information Systems", *IEEE*, Vol. *5*(1), pp 36-44.
17. Krejcie, Robert V., Morgan, Daryle W. (1970), "Determining Sample Size for Research Activities", Educational and Psychological Measurement.
18. Kumar, R. (2011), "Research Methodology, a step-by-step guide for beginners". SAGE Publication, Singapore.
19. Kumar, R. L., Park, S., & Subramaniam, C. (2008)", "Understanding the value of countermeasure", ICT Journal, pp. 80-89
20. Papadopoulou, P., Kanellis, P., & Martakos, D. (2000), "Trust formation in e-commerce relationships, Paper presented at the 7th Research conference, Spain
21. Sekaran, U. (2006), "Research methods for business: A skill building approach." John Wiley & Sons, UK.
22. Siponen, M. T. (2000), "A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, Vol. *8*(1), pp 31-41.
23. Siponen, M. T., & Oinas-Kukkonen, H. (2007), "A review of information security Issues and Respective research contributions, *ACM Sigmis Database*, Vol. *38*(1), pp 60-80.
24. Stephanou, A. T., & Dagada, R. (2008), "The Impact of information Security Awareness Training on Information Security Behaviour: The Case for Further Research." Information Security, South Africa.
25. Straub, D. W., & Welke, R. J. (1998), "Coping with systems risk: security planning Models for Management decision making", Management Information Systems Q*uarterly*, Vol. *22*, pp 441-470.