https://doi.org/10.48009/1_iis_2011_271-297

Issues in Information Systems

Volume XII, No. 1, pp. 271-279, 2011

IDENTIFYING INFORMATION SECURITY GOVERNANCE DIMENSIONS: A MULTINOMIAL ANALYSIS

Sushma Mishra, Robert Morris University, mishra@rmu.edu
Jay Powell, Founder and CEO, Better Schooling Systems, jpowell@tir.com

ABSTRACT

The purpose of this paper is to identify broad dimensions of information security governance (ISG) that lead to developing an effective security program. The main contribution of this paper lies in establishing a mechanism using multinomial analysis on qualitative data. A value focused *analysis is conducted to develop 23 ISG objectives. A multinomial analysis is performed on the data to identify underlying dimensions of ISG. Results suggest three dimensions of ISG and its interrelationships. The contributions are discussed and future research directions are presented.*

Keywords: Information security governance, value focused thinking, multinomial analysis

INTRODUCTION

The Information Systems Audit and Control Association (ISACA) have defined information security governance as a set of responsibilities and practices that are exercised by the executive management to provide a strategic direction such that risks are managed appropriately and an organization's resources are used responsibly [11]. IFAC and ISACA also note that in order to ensure information security, it needs to be considered in the context of enterprise governance. This is because security governance sets the tone for adequate information security policies and practices [1]. While the relationship between good governance and information security has been noted in the literature [10, 25] there has been little guidance as to how "good" *enterprise* security governance can be achieved and what are the broad dimensions leading to good security governance practices.

Emphasizing the importance of right objectives for governance, Brotby (2009) suggests that "governance requires defined objectives to know what we are to manage (pg 27)" and these objectives serve as the reference point for meaningful management metrics. While [29] notes, "each firm's governance structure will be unique to its objective and performance goals" (pg 14), yet a generic set of objectives are necessary for ensuring a good strategic direction for the governance program [3]. The obvious questions that arise are:

- What are the objectives for *enterprise security governance*?
- What are underlying dimensions for good security governance practices and what is their interrelationship?
- How can the objectives for *enterprise security governance* defined?

In his paper we use value-focused thinking to define objectives for *enterprise security governance*. The new use multinomial analysis to our interview coded data identifies the clusters or dimensions of ISG and its interrelationships. Using the multinomial procedure on the developed ISG objectives, we propose three dimensions of ISG: Resource, Ethics and Training. These dimensions are the important for developing effective information-security governance program.

The remainder of this paper is organized as follows. The section following the introduction reviews the extant literature in this area. The subsequent section presents the theory and methodology portion of this work. Following the theoretical underpinnings, a discussion is generated on the dimensions proposed in the study. The implications and contributions are presented and future research directions are suggested. The last section presents the conclusion of the study.

LITERTAURE REVIEW

Technical ISG Research

This body of research largely comes from the technical security requirements of a system, i.e. confidentiality, integrity and availability of data. From enterprise security governance perspective, the need is to identify the corresponding governance requirements. While confidentiality as a requirement may be pertinent, it can only be assured if there are proper access control structures. Some of the prominent technically oriented models are discussed below.

International Standards Organization joined hands with International Electrotechnical Commission (IEC) for developing a series of standards for Information Security Management (ISM). ISO 17799, renamed as ISO/IEC 27002, is a prominent information security governance framework with a technical orientation to security management. These standards, also known as ISO/IEC 27000 (ISO27K) series of standards. ISO/IEC 27002 are the best practices for security management and are widely used information security management framework in North America and Europe.

The framework provides guidance about security in 11 different areas. It is exclusive to information security, and only addresses that issue. The framework is divided into 10 sections, with 36 objectives [9]. The framework provides much more guidance on precisely 'how' things must be done [25]. ISO/IEC 27002 is, in many cases, the framework of choice of IT and information security managers because of its technical superiority [25]. With similar orientation, Information Technology Infrastructure Library (ITIL) is a widely used framework for referencing security management principles.

The framework was developed in UK by the Office of Commerce. It identifies a broad range of processes that are considered as best practices for information technology service management. ITIL provides security from the service provider perspective, identifying the relationship between security management and IT security officer [12]. However, there are many challenges which emerge while implementing ITIL in organizations as it brings about sweeping changes in an organization in the form of changed processes and culture [12]. It is difficult to assess the "value" that is added by implementing these changes.

Occurrence of business risks is becoming imminent as the corporate network, processes and critical business data are vulnerable to attacks from the Internet [22]. Qiang and Hua-ying (2007) argue that Internet security governance is an iterative and continuously evolving process. Finne (1996) proposes an information security chain model for security management in an organization. The model comprises twelve modules and eighty sub modules, each emphasizing an area of security management.

In technically oriented enterprise security governance research, security architecture is considered a crucial aspect of governance. From this perspective, researchers use security objectives as overarching access control, enterprise architecture and authentication rules for a computer system [21, 30]. Booker (2006) argues that it is important to maintain a database of critical network and information assets for effective information security governance and propose a security management model. The model consists of five components. The model suggests that professional security operations must deliver security for the IT environment with appropriate value, service levels and accountability to the top management of the enterprise.

Socio-organizational ISG Research

This research is based on the importance of policies, procedures and controls for providing the overall security environment in an organization. Research in this area emphasizes the importance of formalized procedures and individual inputs in the enterprise security governance process. There are several existing frameworks for information systems security governance, in research and in practice, that advocate the socio-organizational approach to security management.

Control Objectives for Information and Related Technology (COBIT) provides guidance on management's role in security management. It is the most widely used information technology (IT) governance standard in United States. The framework provides "good practices" across a domain and a process framework that presents activities in a manageable and logical structure (ITGI, 2007). COBIT helps an organization align its business goals with IT goals.

It emphasizes the importance of business needs that are satisfied by each of its objectives. The framework divides IT processes into 34 types and categorizes these into four domains:

- Plan and Organize,
- Acquire and Implement,
- Delivery and Support, and
- Monitor and Evaluate.

These domains contain 34 high level control objectives and 215 sub control objectives.
Along similar lines, Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework also describes a unified approach for evaluation of the internal control system that a management designs with the objective of achieving reasonable assurance of the fundamental business objectives. The COSO framework suggests five control components:

- Control environment,
- Risk assessment,
- Controls activities,
- Information and communication and
- Monitoring.

The model suffers from a myopic view of security threats and is more concerned with data security than formal or informal level of organizational vulnerabilities.

Development and use of security polices for effective governance is heavily researched from socio-organizational perspective of information security governance. There have been several calls in the information security research literature to aid information security policy formulation [23]. Straub (1990) uses general deterrence theory to facilitate security policy formulation. Moultan and Cole (2003) emphasize the importance of sound security policies as being vital for a security program and provide guidelines for development of internal controls [26]. These authors categorize security governance on the following dimensions: responsibilities in practices, strategies and objectives, management,

- Resource management,
- Regulatory compliance,
- Policies and procedures and
- External communication.

Along the same lines, Eloff and Eloff (2005) suggest a comprehensive approach towards information systems security governance with well managed controls to minimize risk and ensure effectiveness and efficiency.

Security policies, standards and procedures are also highlighted in Information Security Architecture (ISA) model proposed by Tudor (2000). The model proposes that all individuals should know their responsibilities with regard to protecting the organization's resources.
McCarthy and Campbell (2001) also emphasize the role of security policies in their proposed Capability Maturity Model (CMM) approach for security governance. The uniqueness of the model is its assessment of the current information security capabilities for architect in an appropriate security solution. The main criticism of this approach lies in the anecdotal nature of the model and lack of theory or empirical validation to lend it credibility.

Da Veiga and Eloff (2007) propose an integrated information security governance framework which is a result of triangulation of components of many of the above mentioned models. The main problem of governance models with a policy focus is that little or no emphasis placed on feedback and modification with changing business requirements.

The security governance models with requirement analysis, design, implementation and testing have a solid foundation in the systems approach underlying many IS development and management approaches.
Kolokotronis et al (2002) propose a multidimensional model with following objectives:

- Business needs or requirement analysis;

- Risk and cost assessment;
- Security strategy implementation and
- Monitoring.

These authors suggest that security should be managed at a corporate level and not at the local level to solve specific technical problems.

Moultan and Cole (2003) present a similar argument in support of treating security governance as an enterprise issue to establish an adequate control environment. It is important to identify risks so that management can assign responsibility to the right people to develop and implement appropriate controls to mitigate the risk.

Dutta and McCrohan (2002) argue that sophisticated security technologies can be rendered ineffective by the failure to differentiate among critical information assets, poorly designed operating procedures or lax attitudes towards security within the organization. Poole (2006) argues for an information security framework established by combining the best of ISO 17799 and COBIT into an information security benchmarking model. In conclusion, a review of information security governance research suggests lack of empirically developed information security governance objectives and dimensions. This study addresses this gap and develops such objectives.

THEORY AND METHODOLOGY

This research is grounded in *value-focused thinking* as advocated by Keeney [13, 14] and subsequently used by Dhillon and Torkzadeh [5] to define value based objectives. Theoretically *value-focused thinking* is grounded in Catton's (1959) *Value Theory*. In this section, we describe the theoretical and associated methodological aspects of *value-focused thinking* as used to define *enterprise security governance* objectives.

Value Theory suggests that the core values of individuals guide their decision making process. Catton argues that an individual's preferential behavior shows certain regularities and this pattern can be attributed to some standard or code, which persists through time. Values provide a basis by which people can control their "intensities of desiring various desiderata" (something desirable).

This approach provides a theoretical platform to affirm that values are important for decision making. Incorporating values in developing decision objectives significantly helps individuals accept the results of such decisions. This thinking has significantly influenced the management science and decision making literatures. Keeney (1992). For instance, argues that values are guiding principles to evaluate the desirability of a particular consequence. He notes, "values are what we care about and they should be the driving force for our decision making" (Keeney, 1992, pp. 3).

Values are principles for evaluation, which we use to evaluate the actual or potential consequences of action and inaction of decisions. Keeney (1992) suggests that value focused thinking is a better way of making decisions especially if there are many subjective interpretations involved. A detailed discussion and comparison between value-based and alternative-based thinking is beyond the scope of this paper. Further details can however be found in Keeney (1992).

A. Steps in conducting value-focused thinking

Following {Keeney, 1992, 1999) in this research, we used the following three steps to arrive at value-based objectives for *enterprise security governance:*

Step 1. *Develop a comprehensive list of personal values underlying the problem being explored*.

The primary researcher undertook extensive interviews, using relevant probes to elicit underlying values of respondents.

Step 2. *Change the values enlisted to a common form and convert them into objectives.*

The data collected in step one is collated and presented in a common form, which enables cross comparison and easy interpretation. Values are systematically changed to objectives by adding directional preferences.

Step 3. *Classify the objectives as means and fundamental for the decision context.*

Objectives are clustered into groups and then classified into *fundamental* and *means* using the WITI (*why is this important)* test.

The process of identifying the values for *enterprise security governance* starts with extensive interviews. In this study, 40 interviews were conducted with a diverse group of people representing 9 different industries and various functional areas. Some of the respondent roles that participated in this study are;

- Chief Information Officers (CIO),
- Information Technology Directors, Security Managers,
- Security Officers,
- Systems Auditors and Helpdesk
- IT specialists,
- HR managers,
- Accounting Manager.

The respondents had at a minimum of 5 years of professional work experience and significant experience of using IT systems. The values thus generated were converted into common form, which are then converted to objectives by adding a directional preference.

As suggested by Keeney (1992), an objective has three features, a (an):

- Decision context,
- Objective and
- Direction of preference.

By adding a verb to the common form of value statements provided a directional preference and converted it into a decision objective. From the list of values, 180 objectives were developed. The researchers did the creation of objectives intuitively in an iterative manner, where the emerging themes from the values were captured and labeled conceptually.

Using the WITI (Why Is This Important) test (Keeney, 1992) all clusters are further classified into *means* and *fundamental categories.* A cluster of objectives that leads to another objective being considered in decision-making is a means cluster of objectives whereas a cluster of objectives which is fundamental and important in its own right in a decision making process is called fundamental cluster of objectives.[1]

Applying the WITI test, categories of means and fundamental objectives are created and their interrelationships were established. This step calls for conceptually differentiating between means and fundamental objectives. The application of WITI test to all the objectives resulted in six fundamental and seventeen means objectives for information security governance (See table 1 Appendix A). An excel sheet with all the objectives as columns and respondents in rows was created. Based on the interview data, each interviewee's response was coded in the sheet (1=when the particular interviewee contributed to the objective, 0=when the interview did not contribute to the objective). This enabled us to perform multinomial procedure on the newly created excel data sheet.

Multinomial Procedure Works

The purpose of this procedure is to identify *strong* associations among categories within or between one or more data sets. It is a novel procedure, using an adaptation of the multinomial statistic The result is a new statistic of the order of σ or μ, which its developers are calling Thurs (ρ). It represents the proportion of explained variability within a cell compared with the total possible variability that cell contributes to the entire data matrix. It can be read by its name or as "proportion of explained variability." This symbol, having an appearance to the Roman letter "p" was used because both lower and upper case "Ps" already have statistical meanings. This procedure had its origins [19] to bypass the problem of including linearly dependent variables in analysis. It applies only to frequency data,

[1] The aim of this paper is not to propose new objectives for ISG but how to use multinomial analysis on developed objectives for hidden clusters. The detailed discussion about developed objectives and its implications is beyond the scope of this paper.

but is applicable to both qualitative data and quantitative data or crosstabulations of these two data types. In this particular instance, it is applied to qualitative data.

The procedure:

1. We begin by crosstabulating the frequencies in the data set(s).
2. We collapse the entire matrix sequentially around each cell within it, providing a cell-by-cell analysis of the matrix.
3. We determine the minimum possible value for the cell being examined. In most cases, this will be zero (0).
4. We determine the maximum possible cumulative probability in that cell and the corresponding value for the observed frequency or less.
5. These two accumulations are then compared by dividing the maximum sum into the observed frequency sum. The magnitude of the quotient ($\not{p}$) represents the strength of the association between the collated categories.

Specific to this study:

1. The frequencies of the characteristics of the interviewed managers were crosstabulated by these characteristics, producing a diagonally symmetrical frequency matrix.
2. The Thurs ($\not{p}$) values were obtained independently for each cell in the matrix.
3. These were sorted in descending order of magnitude.
4. Since this was the first application of this procedure, the magnitude of the measurement error from these data is unknown. We used an arbitrary $\not{p} \leq 0.900$ (This statistic has a potential range of $0.000 \leq \not{p} \leq 1.000$.)
5. The frequencies of these high associations were counted by category and the matrix was reordered from high to low according to this count. This cluster analysis was conducted by hand using the data from an Excel® spreadsheet.
6. The three highest characteristics, by frequency that seemed to stand mainly alone, were made the centroids of the three clusters developed. Visual inspection and þ magnitude were used to construct the Venn diagram. It is now possible to test the major cluster analysis procedures to determine which of the produces very similar results. If all fail, a new algorithm will be prepared and a novel clustering procedure will have been established.
7. The hand-operating procedure was used to maintain intellectual control of the process.

CLUSTER INTERPRETTATION

The multinomial procedure described above was applied to the table and the resulting $\not{p}$ values are provided below the frequencies. Notice that the magnitude of the $\not{p}$ values does not coincide with the magnitude of the frequencies. This procedure extracts nonlinear relationships. Since we do not yet have a solution for the standard error of this statistic, we have set arbitrary limits that seem to make sense of these data. As indicated on Table 1, we set two levels of importance for the strength of the connection observed. We regarded a strong connection as representing $1.0000 \geq \not{p} \geq 0.8995$, which rounds to 0.9 to the third place. These connections did not accommodate all the variables, so we regarded as connected a second level $0.8994 \geq \not{p} \geq 0.7995$, which picks up the next 10 %. This move brought data clarity (M5) into a connection with cohesiveness (M11), making it possible to represent every variable. The heavy arrows show the strong connections and the light arrows show the remaining connections.

Figure 1 provides a pictorial version of the results. These clusters were produced by hand, as we do not yet an algorithm to use the þ statistic in a centroid clustering procedure. The clusters were defined by the strong connections and then filled in with the remaining connections.

Three clusters emerged, with Ethics being the centroid for the cluster with the most frequent strong connections. This cluster was followed by Resources, which also had many interconnections with the Ethics cluster. The third one centered upon Training, which had no strong connections with the other two.

Figure 1: Dimensions of Information security Governance

A. Cluster 1: Ethics

The Topic of Ethics (M16) had all six connections strong. We, therefore, made it the centroid of the main cluster. In addition, many of these five of these six, Alignment (M4), Leadership (M10), Cohesiveness (M11), Sanctions (M6), Trust (M17) and Awareness (F2) had mutual connections as well. Alignment and Trust did not connect with Awareness; Leadership did not connect with Sanctions. Many of these connections were strong.

The components of the Ethics cluster appear to include the tasks provided in a corporation by management. Data Clarity (M5) seems to be the orphan of this set. Is this characteristic of IT departments in business? The weakest component of this group of attributes is awareness. This observation is reinforced by the fact that none of the seven had a link to Communication (M3). This observation could mean that the corporate culture tend to have the management team operating in isolation from the balance of the organization. This observation requires further study to confirm this indication of possible dyfunctionality. If it is supported, this procedure could prove to be a useful tool for identifying corporate strengths and weaknesses.

B. Cluster 2: Training

The cluster that focuses around Training seems to contain many of the functions or the HR department of many corporations. Although Leadership has no strong connections with the second cluster, with only two connections overall, it seemed reasonable to use Leadership as the link between management and the HR department. This area of a business seems to be the place where the longevity of any corporation is obtained and maintained.

Does the lack of a strong connection between Accountability and Leadership and the absence of such a connection between accountability and Ethics give an accurate picture of corporations as represented by the 52 interviewees?

The structure of this cluster appears to be very loose. The critical four-way connection among Training (M15), Communication (M3), Improvement (F5) and Accountability (F6) is strong. Improvement and Assessment (M8) are also strongly linked.

Feedback (M9) is linked to Clarity (M2) Efficacy (M1), Accountability (F6) and Control Clarity (M7) but not to Assessment (M8) and not to Leadership. In the absence of these last two links, it is difficult to see how the HR department can fulfill its function establishing and maintaining performance quality. This group appears to know

what it is doing with respect to internal clarity of operation. However, the amount of disconnect with central management suggests that it may not be fulfilling its role effectively through no fault of its own.

C. Cluster 3: Resources

The Components of this cluster appear to be related to the day-to-day operations of the business. These range from Trust (M17) to Standards (M14), Strategy (F1), Policy Clarity (F3) and Commitment (M12) to Compliance (F4).

Commitment is strongly related to Awareness and Sanctions, while Compliance is disconnected from Commitment and instead is strongly related to Standards less strongly to Trust. The inference seem to be that the rank and file of the employees are expected to do as they are told and not seen as a resources for creative input to management.

The cluster is loosely knit with important linkages missing, such as between Commitment and Compliance or Sanctions and Compliance. There is a connection, however between Accountability and Compliance. Is this an indication that a major role of the HR department is to enforce the conditions of the contracts for employment?

D. Implications

This paper has applied a non-linear approach to the analysis of qualitative (interview) data. The image that has emerged is that of a company that seems to be operating in the typical business paradigm of a tightly knit and dedicated management team surrounded by a loosely knit group of more or less indifferent employees.

Once again, this procedure for identifying relationships within a business enterprise that attests to the health of the venture. Most of the other connections or lack thereof, seems to make intuitive sense.

Further study will be needed to determine whether this novel nonlinear approach to qualitative data provides a more accurate picture of the structure of the corporations being studied than the more usual procedures. Confirmational studies will be needed to establish the accuracy of the diagnostic value of this procedure.

In our plans, we propose to cluster the interviewees and then see how the management personnel's map matches the structural map produced here. We will be looking for matching or mismatching of attitudes and skills to determine whether this map accurately describes the cultural structure of these corporations. If it does, the procedure may prove to be a new tool for the analysis of qualitative data.

CONCLUSION

In this paper, Value Focused Thinking and multinomial analysis has been used to propose three dimensions of effective information security governance. A clear understanding the dimensions of ISG and the underlying objectives of these dimensions would lead to a better information security governance program in an organization resulting in more security information systems. Theoretically, this paper contributes to information systems literature by proposing four dimensions of ISG which are theoretically grounded and empirically developed. There is little research in this area especially with almost non-existent work on empirically driven ISG objective sand dimensions. From practitioner viewpoint, this research can help in better information security governance preparedness in organizations based on the dimensions proposed.

Organizations can assess its preparedness on the each of the dimension and implement the dynamics if the proposed dimensions in practice. This research also contributes methodologically. Use of VFT has been done in information systems before (Dhillon and Torkzadeh, 2006) but using multinomial analysis on objectives developed through VFT is not a common thing in IS.

This study provides a new way of combining qualitative and quantitative techniques to a problem. Use of multinomial analysis in IS research can significantly help our discipline by using not so common techniques to study the problems in this discipline.

REFERENCES

1. Allen, J., and Westby, J.R. "Characteristics of Effective Security Governance ", Carnegie Mellon University, Software Engineering Institute, CERT®
2. Booker, R. "Re-engineering enterprise security," Computers & Security (25) 2006, pp 13-17.
3. Brotby, W. (2009) Information Security Governance: Guidance for Information Security Managers, IT Governance Institute
4. COSO "Putting COSO theory into Practice: Tone at the Top," Committee of Sponsoring Organization of the Treadway Commission Retrieved on 10/10/08 www.coso.org
5. Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.
6. Eloff, J.H.P., and Eloff, M. "Integrated Information Security Architecture " Computer Fraud and Security (11) 2005, pp 10-16.
7. Finne, T. "The information security chain in a company " Computers & Security (15:4) 1996, pp 297-316.
8. ISACA "CISA Review Manual," Information Systems Audit and Control Association, Rolling Meadows, IL, 2004.
9. ISO "ISO/IEC 17799:2005," International Organization for Standardization 2005.
10. ITGI, and OGC "Aligning CobiT, ITIL and ISO 17799 for Business Benefit," Information Technology Governance Institute and Office of Governement Commerce, pp. 1-62.
11. ITGI (2003) IT Control Objectives for Sarbanes-Oxley. IT Governance Institute, Rolling Meadows
12. ITIL "ITIL V3," 2007. Retrieved on 10/10/08 http://www.itlibrary.org/
13. Keeney, R. Value-focussed thinking: a path to creative decisionmaking Harvard University Press,Cambridge:Massachusetts, 1992.
14. Keeney, R. (1999) The Value of Internet Commerce to the Customer, Management Science, 45(4), pp 533-542
15. Kolokotronis N, Margaritis C, Papadopoulou P, Kanellis P and Martakos D, " An Integrated Approach for Securing Electronic Transactions over the Web," *Benchmarking* 9(2), 166-181, 2002
16. McCarthy, M.P., and Campbell, S. Security Transformation McGraw-Hill, New York, 2001
17. Moulton, R., and Coles, R. "Applying Information Security Governance," Computers & Security (22:7) 2003, pp 580-584.
18. Poole, V. "Why Information Security Governance Is Critical to Wider Corporate Governance Demands—A
19. Powell, J. C. & Shklov N. (1992). Obtaining information about learners' thinking strategies from wrong answers on multiple-choice tests. *Educational and Psychological Measurement, 52*, 847-865.
20. European Perspective " in: Information Systems Control Journal, 2006 Sandhu, R., and Samrati, P. "Access Control: Principles and Practice," IEEE communications) 1994, pp 40-48.
21. Segev, A., Porra, J., and Roldan, M. "Internet security and the case of Bank of America. Association for Computing Machinery," Communications of the ACM. (41:10) 1998, pp 81-87.
22. Solms, B.v. "Information Security governance: COBIT or ISO 17799 or both?," Computers & Security (24) 2005, pp 99-104.
23. Solms, B.V. "Information Security-The Fourth Wave," Computers & Security (25) 2006, pp 165-168.
24. Solms, S.P.a.R.v. "IT oversight: an important function of corporate governance " Computer Fraud & Security), June 2005, pp 11-17.
25. Straub, D. "Coping with systems risk: security planning models for management decision making.," MIS Quarterly (22:8) 1998, pp 441-465.
26. Tudor, J.K. Information Security Architecture-An integrated approach to security in an organization Auerbach, Boca Raton, Fl, 2000
27. Qiang, Y and Hua-ying, S, (2007), A Systematic Research and Simulation of the Internet Security Governance,
28. Weill, P. and Ross, J. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Boston, Massachusetts
29. Ward, P., and Smith, C. "The Development of Access Control Policies for Information Technology Systems," Computers & Security (21:4) 2002, pp 356-371