Can IT Security be Improved with Better IT Leadership in the 21st Century University?

Glenn Stewart  
Queensland University of Technology, g.stewart@qut.edu.au

Neil Thelander  
Queensland University of Technology, n.thelander@qut.edu.au

Follow this and additional works at: http://aisel.aisnet.org/amcis2005

Recommended Citation
http://aisel.aisnet.org/amcis2005/461
Can IT Security be improved with better IT Leadership in the 21st Century University?

Glenn Stewart  
Queensland University of Technology  
g.stewart@qut.edu.au

Neil Thelander  
Queensland University of Technology  
n.thelander@qut.edu.au

ABSTRACT

Organizations generally are not responding effectively to rising IT security threats because people issues receive inadequate attention. The stark example of IT security is just the latest strategic IT priority demonstrating deficient IT leadership attention to the social dimension of IT. Universities in particular, with their devolved people organization, diverse adoption of IT, and split central/local federated approach to governance and leadership of IT, demand higher levels of interpersonal sophistication and strategic engagement from their IT leaders. An idealized model for IT leaders for the 21st century university is proposed to be developed as a framework for further investigation. The testing of this model in an action research study is proposed.

Keywords (Required)  
Leadership, CIO, IT Security, Action Research

INTRODUCTION

The latest research identifies that the effectiveness of IT security is more impacted by a lack of attention to people issues such as culture, awareness and education than by security technology which is increasingly available and implementable. Attention to security process issues such as policy frameworks and procedures demonstrate progress, but their effectiveness is conditional on human uptake. Universities, with their devolved organization and distributed IT support, have amplified the challenge of the people issues with security.

Security is but the most recently elevated IT strategic priority to have difficulties of effective response thrown into sharp relief. People issues around IT have generally not been well handled, and the IT industry response has often been to invent more technologies than focus on achieving business benefit. Questions about the effectiveness of IT leadership are raised and make explicit challenges for improvement.

This research paper introduces a new framework of leadership by drawing on the observations the requirements demanded of the CIO and IT team in the university setting. It proposes an action research program designed to test the efficacy of this framework in binding policy, understanding and commitment to IT security by the business managers. It commences with a review of the policy and leadership needs in the IT Security domain, from which the framework is derived. It closes with the proposed research design.

WHAT IS WRONG WITH IT SECURITY?

Organizations are not responding effectively to rising IT security threats because people issues appear to receive inadequate attention. Kvavik and Voloudakis (2003), Lane (2004), Lane and May (2004) show that the effectiveness of IT security is more impacted by a lack of attention to people issues such as culture, awareness and education than by security technology which is increasingly available and usable. Security process issues such as policy frameworks and procedures may improve matters, but their success appears conditional on human understanding and uptake. Universities, with their unique culture, devolved organization, and distributed IT support, have amplified the challenge of these people issues.

Research in the field of IT security is substantial and growing rapidly due in part to a backdrop of increasing security risk and hence interest. Grayson (2004) describes how increased threats have escalated IT security to the top of IT leader priorities; this is echoed by a recent Gartner Top Ten issue list (Gartner 2004). The Australian Computer Crime and Security Survey (2004) notes several interesting phenomena, of which two are of particular importance to this study:
Few and less organizations reported they were managing security well – 5% down from 11%.

People issues were very important – need for greater senior management engagement (45%), staff training (49%), and user attitudes and behavior (65%).

Kvavik and Voloudakis (2003) summaries key elements in IT security as:

1. Active engagement of senior university management is important to IT security development.
2. There is a significant gap between how importantly IT security is seen by IT staff and the resource priority it is given by the university.

Lane and May (2004) identify five generic critical success factors: top management involvement, information security management structure, policy development and implementation, awareness and awareness raising activities, and culture of compliance. Girard (2004) emphasize the role of the CIO and in developing and maintaining a culture of compliance in order to ensure awareness and proactive approach to IT security and IT priorities.

From this work, it would seem that the role of leadership in stressing the importance of security, and role modeling commitment to a security culture at the highest level is central to IT security effectiveness. The next section examines the wider role of IT leaders.

AN INTEGRATIVE IT LEADERSHIP FRAMEWORK

Broadbent and Kitzis (2004) review the skill set of successful CIOs. They identify new skills and ten key actions for IT leaders to earn a more strategic role in the organization. The first of these is “lead, don’t just manage” and nearly of the others are to do with the effectiveness of the IT leadership team, and its contribution to the broader leadership of the organization.

Collins (2001) reports analysis of detailed observations of long term high-performing companies and identifies key strategies of successful leadership: a focus on natural talent; passionate interest and well rewarded activity; a culture of discipline; the use of technology as accelerator, and stamina for work. People come first and their efforts good or bad are amplified by process and technology.

Lane (2004) identifies key foci for CIO effort in role definition, effective communication, appropriate organization and governance, architecture development, planning, infrastructure, workforce development, emphasizing business value, and developing appropriate metrics. The critical skills for CIO’s appear to be good interpersonal skills and relationship development. Mingay (2004) focuses on repositioning the IT leadership team by restriking the balance between cost cutting and innovation, and developing purpose, trust and relationships.

An idealized model of IT leadership for the 21st century university is proposed as a framework for further investigation. Attention to people and process is the first order issue for IT leadership. IT leaders should be highly interpersonally effective and well connected in alliances and partnerships, with each other and across the university, with the executive leaders and other functional leaders of the university and the staff they represent, and with parties external to their universities who bring value.

The means to effectively engage with people, to create a shared sense of purpose and to ensure that these elements have been communicated throughout the organization have been described by Bass and Avolio (1996, 1999,2003) in their full range leadership model. Augmented by the work of Goleman (1998,2000) on emotional intelligence, these theories assist in developing pragmatic skills in leaders as well as establishing normative benchmarks. This has been articulated by Bartos (2004) where he argues that emotional intelligence is a necessary condition for effective IT team leaders. The relationship between the Full Range Leadership Model and Emotional Intelligence has been examined by Burbach, Barbuto, and Wheeler (2003), and Burbach (2004) who show that emotional intelligence at least enhances and may be a necessary component of transformational leadership. They also observe that the combination may be necessary in order for long term behavioural change to occur (quoting House and Aditya 1997), which is the desired outcome for more effective IT security.

Drawing on these theories, we see that IT leaders should possess flexible styles and rich interpersonal skills to be more effective in supporting their university in ubiquitous use of IT, by engaging with these people and processes that weave the university fabric of teaching, learning and research. They should be able to foster a sense of shared purpose, mission and values. They should be able to instill a culture of problem solving and innovation, tempered by an understanding of the need
to identify, implement and adhere to appropriate security policy and practice. They should be effective in building and sustaining relationships throughout the organization, and pay particular attention to the interactions between the technical team and the business team. This attention to communication flows is paramount for successful transmission of policy. The work by Avolio and Berson (1999) is of particular use in understanding this communication pattern.

PROPOSED ACTION RESEARCH PROGRAM

The action research approach will be used in order to test the efficacy of the model in a real business situation. The research question is “What critical actions should university leaders take to empower their IT security?” The study design is informed by the work of Stewart and Gable (2001), and Baskerville and Wood-Harper (1996) who identify three characteristics of the ideal domain for action research: the researcher is actively involved; knowledge obtained can be immediately applied; and “the research is a cyclical process linking theory and process”.

One of the authors of this paper is the CIO in a university setting, who is setting the agenda, interacting with all key staff and is passionate about improving IT efficacy. Senior executive involvement and support for the study has been obtained. The study has been designed with the intent of an evolving framework of ideas, while applying the theories of effective leadership in the area of IT security. Each cycle will take an action, reflect on its outcomes using participants as informants, and generate findings which will guide the next iteration. Perry and Zuber-Skerrit (1991) state that there are three components to an action research project: a group of people working together who are involved in a cycle of planning, acting, observing and reflecting on their work more deliberately and systematically than usual; and generate a public report of that experience. This project will achieve each of these objectives as follows.

Phase 1 is developing better IT leadership practices which are effective in communicating intent and establishing effective relationships. This leadership development work has commenced. The target audience for this training is the IT executive. In addition, a series of relationship and shared vision workshops will be conducted between the IT executive and the business executives of the university. This work commenced last year, and is continuing throughout the year, using the fishbowl approach. Security policy has been reviewed and new strategies identified. An initial model of IT leadership has been developed which sees the federated group of IT leaders interacting across the university in horizontal IT portfolios.

Phase 2 is studying the promulgation of security policies and their implementation. This will be tracked in terms of the understanding of and adherence to these policies by both the IT and business communities. The attitudes of the senior staff in these groups will be tracked through focus groups, interview and survey. The effectiveness of communication paths and informal networks will be qualitatively assessed. Informal networks will be modeled following the socio-metric approach used by Schenkel, Tiegland and Borgatti (2001). Finally, key participants will be asked to maintain a reflective log, from which attitudes and understandings of the policy will be determined. This will permit research on the efficacy of the communication and leadership strategies employed in the development, implementation and enforcement of the new IT Security policies.

Phase 3 of the study will be the analysis of the correlate of IT leadership with IT security success.

The unit of analysis in this study is the individuals who make up the leadership team which comprises of the formal IT leaders and their business partners. This is appropriate in the federated governance model employed in the university. The study will examine the perceptions of both groups: IT and business. These views will be compared and contrasted to give a consolidated understanding of their dynamic relationship in terms of the local leadership sub-cultures.

Action research is appropriate in this context as the principle researcher is very much concerned with improved leadership practices of business and IT executive. The objective of the study is to both understand the dynamic relationship and to ensure that better practices evolve. In addition, the theoretical aspect needs critical evaluation in terms of the efficacy of the evolved model.

CONCLUSION

This action research program will determine the effectiveness of this idealized model of IT leadership. The direct involvement of the researcher as protagonist suggests an iterative and fluid action research cycle enabling direct professional involvement and the research envelope to act as documentation and communication for continuous improvement of IT leadership. The action research is expected to develop into a more emancipatory approach as the senior IT staff involved in the program develop their leadership and take more control.
REFERENCES


4. Berson, Y., & Avolio, B.J. “Linking transformational and strategic leadership: Examining system of high-technology organization in a turbulent environment” Leadership Quarterly 2005


