3-1-2004

Information Security & Shared Leadership

Paul D. Witman
paul.witman@cgu.edu

INFORMATION SECURITY & SHARED LEADERSHIP

Paul D. Witman
Claremont Graduate University
paul.witman@cgu.edu

Abstract

Much research has been conducted to look for predictors of positive information security results. To date, no research has yet looked at the potential relationships between shared and vertical leadership behaviors and security results. This paper proposes an empirical study to measure these factors and results and examine the relationships among them.

Keywords: information security, security outcomes, leadership style, shared leadership, vertical leadership

Background

Do the leadership style and leadership behaviors of the CIO and the CIO's management team influence the effectiveness of and compliance with organizational information security policies? A new stream of management research focuses on "shared leadership" as a predictor of team effectiveness, and has found support for shared leadership's predictive capabilities in certain contexts (Pearce, 2003).

Key research questions that arise, then, in the context of leadership behaviors and information security might include:

- How do shared vs. vertical leadership behaviors among the CIO's management team affect real and reported compliance with security policies?
- Are shared leadership behaviors positively related to greater effectiveness of security practices, and to greater compliance with security policies?
- Do greater amounts of vertical leadership behaviors result in greater compliance with security policies? And is the compliance perhaps more virtual than real – an attempt to protect one's job, but not necessarily corporate assets?

Definitions and terms

Pearce and Sims (2002), and Cox et al (2003) have defined shared leadership as the exertion of leadership behaviors by peers within a team, rather than by the designated vertical leader of the team. Pearce and Sims (2002) studied five different types of leader behaviors, both for shared and vertical leadership models: aversive (punishment), directive (issuing instructions, commands, and goals), transactional (providing rewards and managing by exception), transformational (providing vision, inspiring, expressing idealism), and empowering (encouraging independent action, teamwork, self-development, self-reward).

Pearce reports that, "Three characteristics of knowledge work that are particularly related to the need for shared leadership include: (1) interdependence; (2) creativity; and (3) complexity." (Pearce, 2003, p. 5) Whitman and Mattord (2003, p. 9) note that security is inherently complex, with many interdependencies between organizations and work units to maintain system security. And clearly, given the broad range of vulnerabilities and attacks that are possible (Schneier, 2000, pp. 14-59), a great deal of creativity is required to foresee and defend against them, and to define systems that are both usable and secure (Adams & Sasse, 1999).

Security generally refers to a broad range of functions to manage the safety and integrity of all of an organization's assets – including physical security, personal security, transportation security, etc. Finne suggests that information security be defined such that "when information is threatened, lost, or misused, it is a question of information security." (Finne, 1998)

There are a wide range of vulnerabilities which must be addressed by an organization's security practices. Security risks may be introduced at a number of points in the organization's operations, including physical, technical, and administrative vulnerabilities. According to Saltmarsh and Browne (1983) as extended by Witman (2003), these vulnerabilities include at least the following items, as shown in Table 1:

Table 1 – Types of Vulnerabilities

Administrative	Technical	Physical
Security Management – visibility, communications, resource allocation	Hardware – Emergency power, redundant systems at all levels, key storage	Physical access controls – badges, door locks, etc.
Personnel Security – background checks, personnel policies	Communications – Network, Virtual LAN's, Strong Authentication, Network Scanning, Firewalls, intrusion detection, encryption	Perimeter alarms – including cameras, glass breakage alarms
Procedural Controls – policy and procedure documentation and training	Operating System – Proper patch levels, audit controls, change management, separation of powers, virus protection	Hazard Protections - Smoke, fire, and moisture alarms
Contingency Planning – Disaster Recovery plans and tests	Application Systems – availability, auditability, integrity, reliability	
Proactive and reactive log review	Database Management System – access controls, auditability, encryption	

While leadership at the CIO level is required to mitigate all of these classes of vulnerabilities, it appears that the administrative class, with its personnel-based impacts across the organization, will be most affected by shared leadership practices in the organization.

Scope

The study will focus on the CIO and their direct reports, as the domain under which vertical and shared leadership will be evaluated. We will attempt to get responses from multiple organizations in a range of industries, so as to improve generalizability of the results. By measuring leadership behaviors at this level, we can look for correlations between certain leadership behaviors and the effectiveness of the organization's security policies and practices.

For the initial study, we will aim for medium-sized health care and banking organizations. Both are information-intensive, privacy-oriented, and regulated (though in different ways), and thus will have consistent externally-facing goals for their security outcomes. Both face security issues, though with different risk and threat profiles. We will look for publicly traded or non-profit organizations. Publicly traded or non-profit firms are preferred due to the ease of access to public filings data on financials and other operational issues.

A random sampling of line employees within the organizations will be surveyed to measure security awareness, actual vs. reported compliance with security policies, and understanding of the business motivation for security.

We will specifically attempt to avoid overrepresentation of any one industry type, to avoid the clustering effects that may be caused by within-industry regulatory standards, management controls, etc. We will also hope to find organizations that place responsibility for security at varying levels in the organization, so as to control for that variable in the organizational mix.

Information Security and Leadership Literature

The literature provides a rich source of material on leadership and team effectiveness measures, and on how leadership might influence information security practices. Sivasubramaniam et al (2002) provide an analysis of "team leadership" behaviors and their relationship to team effectiveness, as moderated by their impact on "group potency". Pearce (2003) suggests that

shared leadership behaviors are most appropriate and effective in contexts involving interdependence, creativity, and complexity of the work tasks.

Whitman & Mattord (2003, p. 20) note that information security systems need a management champion in order to succeed. Gaunt, while focusing on the UK health care industry, also notes the need for leadership to create a security-oriented culture in an organization, noting particularly "The most important influence on staff attitude is a demonstration of the commitment to security by key opinion formers in each staff group." (Gaunt, 2000, p. 154)

Adams and Sasse (1999) looked at the issues around people and information security, and note that systems need to be designed to make them easy to use safely, and that users need to be educated about the need for, and impact of, security policies and practices. In their recommendations, they suggest that "system security needs to be visible and seen to be taken seriously by the organization." (Adams & Sasse, 1999, p. 46) Dhillon, alone and with others (Dhillon, 2001; Dhillon & Backhouse, 2001; Dhillon & Moores, 2001), has written numerous articles about the social aspects of information security, requiring vigilance and compliance from all line employees to maintain effective security.

Insider attacks are a significant risk as well. Magklaras and Furnell (2001) have created a tool to evaluate the probability of IT misuse from inside the organization. Dhillon and Moores (2001) has looked, at a theoretical level, at "the enemy within," quoting Parker's study that as much as 81% of computer crimes are committed by insiders (Parker, 1991). This rate of insider-driven crimes gives special emphasis to the need to examine the impact of shared leadership on individual line employees' attitudes and behaviors as it relates to information security – both at the end user level, and at the system administrator level.

Security outcomes will be operationalized via a variety of measures, leveraging ISO Standard 17799 (Calder & Watkins, 2002) as a base for evaluation. An overall organizational survey instrument, like that utilized by the Human Firewall Council (2003), will measure the organizations' security management practices. ISO 17799 focuses on ten aspects of information security, as summarized by The Security Policies and Standards Group (Group, 2001), including:

1. **Security policy** - This provides management direction and support for information security
2. **Organization of assets and resources** - To help manage information security within the organization
3. **Asset classification and control** - To help identify assets and appropriately protect them
4. **Personnel security** - To reduce the risks of human error, theft, fraud or misuse of facilities
5. **Physical and environmental security** - To prevent unauthorized access, damage and interference to business premises and information
6. **Communications and operations management** - To ensure the correct and secure operation of information processing facilities
7. **Access control** - To control access to information
8. **Systems development and maintenance** - To ensure that security is built into information systems
9. **Business continuity management** - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
10. **Compliance** - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement

The Human Firewall Council tool, or a derivative of it, might provide a basis for measuring an organization's security management practices, and the compliance to them. There is a dearth of academically validated survey instruments in this area, and that will likely be one of the contributions of this study.

The Human Firewall Council also offers a worker-oriented survey, that "measures security awareness levels of your organization's employees" (Council, 2003). This survey may be used as a foundation for development of a worker-oriented survey instrument. Furnell et al, in an article on information security in the health care sector, describe a survey instrument used to assess staff attitudes and staff culture as it relates to information security (Furnell et al., 1997). Finch et al write on a similar topic, looking at a more general range of businesses (Finch et al., 2003), and published a detailed survey instrument

(Finch, 2002). These instruments, likewise, could provide a basis for creation of a survey instrument focused on line employees and compliance concerns, and are included as an Appendix.

Hypotheses

Key independent variables are hypothesized to be the measures of leadership behaviors as identified in the Pearce & Sims (2002) instrument. This instrument is expected to be used with the CIO and the CIO's direct reports, to evaluate leadership behaviors amongst the members of that team.

Control variables will include organization demographics (size, industry), reporting levels of CIO and CSO, and level of e-commerce enablement (brochureware, extranet, transactional capabilities, etc.), as an indicator of the level of direct exposure of systems to attack from outside.

Key dependent variables will focus on the results of the organization's information security function, including its ability to achieve compliance with policies as reported at the management level, at the system administrator level, and at the line employee level.

Based in large part on Pearce and Sims' work, the following hypotheses will be tested in this study:

Hypothesis 1: Vertical leadership behaviors are an important predictor of positive performance results in security.

Pearce and Sims found moderate support for this type of hypothesis in their study of Change Management Teams. Based on the understanding that leadership and management support are prerequisite to positive performance in security (Whitman & Mattord, 2003, pp. 31-33), this seems to be a likely scenario. In addition, it seems likely that shared leadership, given that it was an important predictor of success in the Pearce and Sims study, would also be an important predictor of positive performance results in security:

Hypothesis 2: Shared leadership behaviors are an important predictor of positive performance results in security.

Dhillon and Moores (2001), in looking at internally executed computer crimes, note that the motivation to "succeed" in the organization, as driven by top management direction and punishments, may deliberately or inadvertently override the need for ethical and proper behaviors. These behaviors may then contribute negatively to security results, leading to Hypotheses 3 and 4. Pearce and Sims found marginal support for hypotheses of these two forms:

Hypothesis 3: Aversive leadership is negatively related to performance results in security.

Hypothesis 4: Directive leadership is negatively related to performance results in security.

Finally, Pearce noted that some leadership behaviors can result in people doing or appearing to do what is right and expected. "People search for cues about what is and what is not rewarded in their organizations. They subsequently engage in (or at least create the appearance that they engage in) those behaviors that they believe are rewarded." (Pearce, 2003, p. 12-13) From this foundation comes the final hypothesis:

Hypothesis 5: Aversive leadership behavior is negatively related to the relationship between actual and reported security policy compliance.

Research Methodology Overview

Based on the fact that the study appears to have a theoretical grounding, and that various survey instruments covering parts of the study concepts already exist, the study is a good candidate for a fixed research design (Robson, 2002, p. 95-96). The research will utilize the survey instruments to gather data about organization and individual demographics (control variables), leadership behaviors, and security outcomes.

The survey instruments will be created in three variations: one to focus on the CIO and the CIO's direct reports, a second to focus on system administrators, and a third to focus on line employees. For each survey instrument, the questions will be evaluated and adjusted based on their ability to provide data to answer the proposed research questions (Robson, 2002, pp. 241-246).

Each survey instrument will be pre-tested with an appropriate audience (Robson, 2002, p. 254). The purpose of the pre-test is to confirm the correct wording of the questions, to confirm that the appropriate data is being collected, and to make the survey questions more effective at gathering the required study data. The survey results will be examined statistically to look for overlapping questions, and to eliminate those that do not provide additional value or that reduce construct validity. This process helps to address the overall internal validity of the study, ensuring that the study data is internally consistent. In addition, the questions will be structured to provide multiple indicators of key constructs, improving reliability (Neuman, 2003, p. 181).

Organizations will be chosen for the study in a purposive fashion, seeking specific types of companies as noted in the discussion of the study's scope, above. Survey samples will be chosen differently for each survey group within a given organization. At the CIO and direct report level, the sample will be exhaustive, with the intent to collect data from all members of those groups within the study companies. Sampling at the administrator level will be random, with the sample size driven by the number of administrators within that particular company. Finally, at the end user level, the sampling will be a stratified random sample, taking random samples from each key line organization of end users. In this fashion, the study would not risk missing key line organizations in the samples (Robson, 2002, p. 262).

Generalizability, or external validity, of the results will be limited by the sampling at the organization level, of the types of organizations studied. Future studies may expand the range of organization types and demographics to create a more generalizable result set.

Directions for Future Research

One key task to accomplish in this study will be to develop and assemble a comprehensive survey instrument that addresses both leadership and security results at the CIO team level. In addition, an instrument to measure policy compliance at the individual level is also required. Using the Pearce & Sims (2002), Finch (2002), and Human Firewall Council (2003) materials as a base, we believe this is a viable goal, and that we have a solid foundation to build on.

Much has been written about the influence of ethics in the abuse and misuse of computers, and in computer security. For example, Loch extends the Theory of Reasoned Action to look at the impact of ethical decision making on various computer use situations (Loch, 1996). Harrington discusses the effect of codes of ethics on information security practices at the individual level (Harrington, 1996), measuring the impact of generic and specific codes of ethics and personal denial of responsibility, on computer abuse. Further research is warranted to examine how codes of ethics might moderate or enhance the effects of leadership behaviors on security results.

Notes:

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Association for Computing Machinery. Communications of the ACM, 42*(12), 40.

Calder, A., & Watkins, S. (2002). *IT Governance: Data Security and BS 7799/ISO 17799* (1 ed.). London: Kogan Page Ltd.

Council, H. F. (2003). *Security Management Index*. Retrieved 11/11/2003, 2003, from http://www.humanfirewall.org/smi/

Cox, J. F., Pearce, C. L., & Perry, M. L. (2003). Toward a Model of Shared Leadership and Distributed Influence in the Innovation Process: How Shared Leadership can Enhance New Product Development Team Dynamics and Effectiveness. In J. A. Conger (Ed.), *Shared leadership : reframing the hows and whys of leadership* (1st ed., Vol. 1, pp. 48-76). Thousand Oaks, Calif: Sage.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security, 20*(2), 165-172.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio- organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security, 20*(8), 715-723.

Finch, J. (2002). *Approaches to establishing IT security culture.* Unpublished MSc, University of Plymouth, Plymouth.

Finch, J., Furnell, S. M., & Dowland, P. (2003, April 23-25, 2003). *Assessing IT Security Culture: System Administrator and End-User.* Paper presented at the ISOneWorld Conference, Las Vegas, NV.

Finne, T. (1998). A Conceptual Framework for Information Security Management. *Computers & Security, 17*(4), 303-307.

Furnell, S. M., Gaunt, P. N., Holben, R. F., Sanders, P. W., Stockel, C. T., & Warren, M. J. (1997). Assessing staff attitudes towards information security in a European healthcare establishment. *Med. Informatics, 21*(2), 105-112.

Gaunt, N. (2000). Practical approaches to creating a security culture. *INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS, 60*(2), 151-157.

Group, T. S. P. S. (2001). *The Contents of ISO17799*. Retrieved 12/05/2003, 2003, from http://www.information-security-policies-and-standards.com/iso17799what.htm

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Loch, K. D., and Conger, Sue. (1996). Evaluating Ethical Decision Making and Computer Use. *Communications of the ACM, 39*(7), 74-83.

Magklaras, G. B., & Furnell, S. M. (2001). Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Computers & Security, 21*(1), 62-73.

Neuman, W. L. (2003). *Social Research Methods: Quantitative and Qualitative Methods* (5th ed. Vol. 1). Boston, MA: Allyn and Bacon.

Parker, D. (1991). Seventeen information security myths debunked. In K. Dittrich, S. Rautakivi & J. Saari (Eds.), *Computer Security and Information Integrity* (Vol. 1, pp. 363-370). Amsterdam: Elsevier Science Publishers.

Pearce, C. L. (2003). The end of leadership as we know it: How combining vertical and shared leadership can transform knowledge work. *Academy of Management Executive*.

Pearce, C. L., & Sims Jr., H. P. (2002). Vertical versus Shared Leadership as Predictors of the Effectiveness of Change Management Teams: An Examination of Aversive, Directive, Transactional, Transformational, and Empowering Leadership Behaviors. *Group Dynamics: Theory, Research, and Practice, 6*(2), 172-197.

Robson, C. (2002). *Real World Research* (2nd ed. Vol. 1). Malden, Massachusetts: Blackwell Publishers, Inc.

Saltmarsh, T. J., & Browne, P. S. (1983). Data Processing - Risk Assessment. In M. M. Wofsey (Ed.), *Advances in Computer Security Management* (1 ed., Vol. 2, pp. 93-116). Bath, Avon, UK: Wiley Heyden Ltd.

Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World* (1 ed.). New York: John Wiley & Sons.

Sivasubramaniam, N., Murry, W. D., Avolio, B. J., & Jung, D. I. (2002). A longitudinal model of the effects of team leadership and group potency on group performance. *Group & Organization Management, 27*(1), 66.

Whitman, M. E., & Mattord, H. J. (2003). *Principles of Information Security* (1 ed. Vol. 1). Boston, MA: Course Technology.

Witman, P. D. (2003, March 7, 2003). *Banking Information Security - How Much is "Enough"?* Paper presented at the SAIS 2003, Savannah, GA.