Winter 12-13-2015

How CISOs Can Become Effective Leaders? A Path-Goal Approach

Gurvirender P. Tejay
Nova Southeastern University, tejay@nova.edu

Markus Winkfield
Nova Southeastern University

How CISOs Can Become Effective Leaders? A Path-Goal Approach

Markus Winkfield
Nova Southeastern University

Gurvirender Tejay
Nova Southeastern University
tejay@nova.edu

Abstract

Information security is a complex issue and Chief Information Security Officers (CISO) are faced with various challenges. Additional research is needed to study the role of CISOs in attaining information security compliance. In this paper, we follow path-goal theory of leadership as a theoretical lens to understand how CISOs can be more effective information security leaders. We present a research model for effective security leadership with emphasis on security member characteristics, organizational environment and security motivation process. This paper suggests that CISOs leadership behaviors must be tailored to communicate and influence subordinates' perception as well as paths to the attainment of information security goals.

Introduction

Information security[1] has shifted from a technical problem to more of a management issue (Herath & Rao, 2009; Von Solms, 2001). In 2014, a Forbes news article reported widely-known corporate data breaches including UPS, JP Morgan Chase, Staples, Sony and Kmart (Hardekopf, 2015). Although these data breaches contain technical factors, they also suggest the need for senior management to be more actively involved. The critical business importance of IT means the failure of information security governance programs can lead to serious personal and corporate liabilities (Von Solms & Von Solms, 2004, 2006).

Chief Information Security Officers (CISO), a relatively new title added to the C-suite, is responsible for a wide-array of information security responsibilities: "facilitating the implementation and ongoing compliance with the multiple domains of the common body of knowledge, such as risk management, operations security, business continuity, and so forth" (Fitzgerald, 2007, p. 262). Unfortunately, CISOs are faced with various challenges related to power, role identity, and employee involvement (Ashenden & Sasse, 2013). In addition, there may be confusion with CISO's responsibilities since CISO may be labeled as a "security manager, security director, or information security officer" (Fitzgerald, 2007). These challenges make it difficult for CISOs to excel as security leaders. In an attempt to build on

[1] For rest of the paper, information security and security will be used inter-changeably.

existing studies (Fitzgerald, 2007; Whitten, 2008; Ashenden & Sasse, 2013), research is needed to understand how CISOs can be more effective security leaders.

Overall, there is also a need for a more active leadership approach and effective communication of information security as a goal (Ashenden & Sasse, 2013). CISOs benefit from IT skills, but they also require soft skills like communication and leadership (Whitten, 2008). Based on experience on CISO job listings, Whitten (2008) found 61% of jobs required communication skills and 39% included leadership skills. These skills are needed for contracts, negotiations, and presentations to convey the difficult cost-benefit of information security implementations. CISOs need to act as change agents and manage how directives are communicated and received by employees (Ashenden & Sasse, 2013). This approach can enhance cooperation when steering groups towards a common information security goal (Koskosas & Asimopoulos, 2011).

CISOs in many corporate environments lack organizational support, and are considered to have one of the most arduous roles for modern business professionals (Perlroth, 2014). CISOs must effectively communicate business problems being resolved and inculcate information security throughout the company to obtain organizational support from employees (Johnson & Goetz, 2007). Building upon this, we argue that CISO's leadership behaviors must be tailored to communicate and influence subordinates' perception as well as paths to the attainment of information security goals. This approach will increase the effectiveness of information security leaders by helping employees actualize the relative worth of security implementations and obtain company-wide support. Not only will this research provide a theoretically grounded approach for understanding how CISOs can excel as security leaders, it will also contribute to a lack of information security research related to goals, leadership, and the role of CISOs.

Literature Review

Information security compliance is a complex issue in organizations (Ifinedo, 2014). Boss et al. (2009) argued evaluating and rewarding individuals for their compliance behavior would increase the degree to which individuals believe controls are mandatory. They suggest employees will adhere to policies that are enforced as mandatory. However, this is a major assumption because even when policies are specified as mandatory they may still not be followed. Vance et al. (2012) argued security non-compliance issues are caused by habit, which means individuals are caught in routine behavior that goes against security policies. But, bad

habits are hard to break. Johnston and Warkentin (2010) highlight the importance of incorporating fear-inducing communication to persuade end-users intentions to follow recommended individual security actions. Later, Johnston et al. (2015) extended the conventional fear appeal model by adding personal relevance with sanctions.

Information security policy compliance issues could be resolved by developing the moral reasoning and values of employees (Myyry et al, 2009). An individual is rationally influenced to comply with security policies based on normative beliefs, self-efficacy, and attitudes (Bulgurcu et al., 2010). Ifinedo (2014) further argued socialization, influence, beliefs and cognition motivate security policy compliance. In addition, personality factors have been argued to be more important than attitudes and intentions (Shropshire et al., 2015). More broadly, Herath and Rao (2009) emphasized the importance of extrinsic and intrinsic motivators to encourage information security policy compliance.

Research suggests a lack of management support is the leading issue in the realm of information security (Von Solms & Von Solms, 2004; Knapp et al., 2006). Top management support consists of leadership, organizational structures, and processes in the protection of corporate information assets (Johnston & Hale, 2009). Although it is often overlooked, middle management also plays an important day-by-day role and might represent the biggest barrier to transforming the organization (Johnson & Goetz, 2007). The involvement of middle management helps spread the responsibility and accountability for information security to lower levels. It can help end-users understand how security applies to their daily operations and enforce training, awareness, and policy compliance (Johnson & Goetz, 2007).

Despite emphasis on top management support, there are limited studies focused on information security leadership. The significant need for obtaining management support and motivating compliance in information security has introduced a need to understand how leadership can help accomplish these goals. There is a difference between management and leadership: management is focused on “controlling”, and leadership is focused on the “creation of a common vision” (Weathersby, 1999). Even though there is no single agreed upon definition of leadership, this research study defines leadership as: “a process whereby an individual influences a group of individuals to achieve a common goal” (Northouse, 2015, p. 5). Information security leaders must overcome organizational challenges and achieve stated security objectives. This paper focuses on information security leadership.

Theoretical Basis

CISOs need to use communication to act as change agents and remove blockages that prevent information security from becoming viewed as only a concern for specialists (Ashenden & Sasse, 2013). Researchers suggest information security should be viewed as a goal to motivate such change in organizational behavior (Koskosas & Asimopoulos, 2011). We take a goal-oriented view that perceives information security as a collection of goals to accomplish in order to manage risks (Oladimeji et al., 2006; Elahi & Yu, 2007; Koskosas & Asimopoulos, 2011). Goals can be used to consciously and unconsciously drive human activities (Koskosas & Asimopoulos, 2011). This view ties in with our aim to understand the role of leadership when communicating information security goals to encourage organizational support in the management of critical information resources.

The Path-Goal theory of leadership serves as the theoretical basis for our study. This theory draws heavily from research on what motivates employees. The Path-Goal theory of leadership examines the relationship between leader behaviors and work outcomes, including subordinate's satisfaction and effectiveness (Evans, 1970; House, 1971; Keller, 1989). According to this theory, leaders initiate structures in the work environment to clarify the path to a desired outcome (Sagie & Koslowsky, 1994). The emphasis is to enable "personal pay-offs to subordinates for work-goal attainment and make the path to these pay-offs easier to travel by clarifying it, reducing road blocks and pitfalls, and increasing the opportunities for personal satisfaction en route" (House, 1971, p. 324).

Although some critics argue the Path-Goal theory has no predictive value and limited empirical support (Schriesheim & Denisi, 1981), other studies point to the contrary and consider it to be a strong framework for understanding leadership effectiveness (Vecchio et al., 2008; Malik et al., 2014). In IS research, Li et al. (2012) empirically found this theory to be useful in understanding how leadership could motivate better development of open source software. The path-goal leadership approach can help us understand how CISOs can effectively communicate information security goals and increase the effectiveness of information security leadership.

Research Model

The path-goal theory contains four major components: leadership behaviors, subordinate characteristics, work environment characteristics, and motivation towards a goal (Northouse, 2015). These components as applied to information security are discussed in rest of this section. The proposed research model is presented in Figure 1.

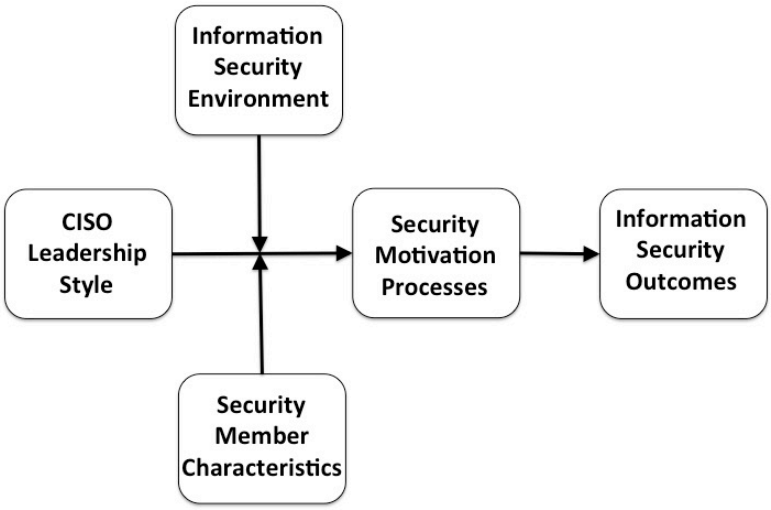

Figure 1. Research Model of Information Security Leadership

CISO Leadership Style. House and Mitchell (1974) listed four primary behaviors related to the path-goal theory: directive, supportive, participative, and achievement-oriented (see Appendix A). Leadership behaviors are pertinent to successful accomplishments in organizations (Holloway, 2012). Research has found leadership behaviors to have a direct effect on an individual's attitudes and behaviors (Momeni, 2009). The attitudes and behaviors of users play a key role in applying protective information technologies (Dinev et al., 2009). Furthermore, the intrinsic and extrinsic factors of attitudes and behaviors influence information security (Herath & Rao, 2009). Therefore, information security goals can be achieved when CISOs use certain leadership behaviors to motivate employees.

Security Member Characteristics. According to House & Mitchell (1975), the subordinate characteristic is a contingency variable that moderates the relationship between leadership behaviors and leadership effectiveness. This characteristic influences how subordinates interpret leadership behaviors (House & Mitchell 1975). The Path-Goal theory states subordinates are more likely to accept leadership behaviors when they perceive the immediate or future satisfaction (House & Mitchell, 1975). For information security, we focus on *Security Member Characteristics.* Individuals have unique characteristics: attitude, motivation, and job satisfaction that are influenced by organizational forces (Vroom & Von Solms, 2004). Due to these characteristics, "the behavior of individual employees plays an important role in the development and evolution of the organizational culture and factors that

affect this behavior to be conducive to information security" (Vroom & Von Solms, 2004, p. 196). Based on concepts of rationality, individuals support decisions that lead to their personal satisfaction (Bulgurcu et al., 2010). Therefore, leadership behaviors that are tailored to the subordinate characteristics and posit the potential satisfaction have the potential to motivate employees towards information security compliance.

Information Security Environment. House & Mitchell (1975) argues that environment factors also moderate the relationship between leadership behaviors and its effectiveness. These factors are outside the control of subordinates but influence their psychological state (House & Mitchell, 1975). The organizational security environment has an influence on employees and internal security operations (Vroom & Von Solms, 2004; Chan et al., 2005). More specifically, organizational design and support for tasks play a role in the security motivation process overall security environment (Vroom & Von Solms, 2004). These characteristics suggest job satisfaction and leadership directiveness determines degree a structure needed to motivate subordinates (House & Mitchell, 1975). Therefore, leadership behaviors that are tailored to the organizational security environment have the potential to motivate employees and increase security outcomes.

Security Motivational Processes. Numerous studies have acknowledged the need for senior security professionals to have strong communication and motivational skills (Johnson & Goetz, 2007; Whitten, 2008; Bradbury, 2011; Koskosas & Asimopoulos, 2011; Ashenden & Sasse, 2013). Faced with a dynamic job role, CISOs must primarily have a firm understanding of how to communicate in both business and technical language (Whitten, 2008; Bradbury, 2011). The technical expertise is not as important as adept leadership skills and business fundamentals (Groysberg et al., 2011). Insufficient communication causes employees to develop their own approach and degrades their ability to understand the value of their support (Adams & Sasse, 1999). Instead of using a one-way approach of authoritatively announcing current security actions, CISOs need to effectively communicate organizational business problems being resolved (Johnson & Goetz, 2007; Ashenden & Sasse, 2013). More specifically, "genuine two-way communication with employees, negotiation and involvement to overcome the often observed 'them' and 'us' relationship, and an acceptance that mistakes and errors will occur" (Ashenden & Sasse, 2013, p. 16). Herath and Rao (2009) argue that extrinsic and intrinsic motivators play a role in information security. However, Son (2011) observed that although extrinsic factors are important, intrinsic factors are more pertinent to

motivate security policy compliance. CISOs can motivate employees by providing coaching and direction, removing obstacles and roadblocks, and making sure security goals are personally satisfying. This approach overtime has the potential to motivate employees and enhance their understanding of security goals.

Information Security Outcomes. According to Dunkerley & Tejay (2009), "organizations require strong leadership that understands how to define information security success within that organizational context, necessitating individuals who understand both information security needs and needs of the organization" (p. 5). Information security leaders will be effective based on how well they lead subordinates goals: employee motivation, employee satisfaction, leader acceptance, and work unit performance (House, 1996). Essentially, CISOs need to communicate and influence subordinates' perception of information security goals, as well as paths to the attainment of goals.

This research article aimed to fill a gap in empirical research by understanding how CISOs can overcome various challenges and excel as effective information security leaders. Based on the view of information security as a collection goals and leadership as an approach to the attainment of goals, the path-goal theory of leadership was used as a theoretical lens to understand how CISOs can be more effective information security leaders. This paper suggests that CISOs leadership behaviors must be tailored to communicate and influence subordinates' perception as well as paths to the attainment of information security goals.

Conclusion

There is a need to discuss what makes CISOs able to define and deliver organizational security goals effectively (Ashenden & Sasse, 2013). The path-goal theory was used as a theoretical lens to understand how CISOs can overcome challenges and excel as information security leaders. We suggest that CISOs leadership styles must be tailored to communicate and influence subordinates' perception as well as paths to the attainment of information security goals. The next step is to gather data from CISOs at large organizations to understand the effect of leadership behaviors, information security environments, and security member characteristics on motivation process and information security outcomes. A present limitation involves leadership behaviors and contingency factors being relevant to all organizational contexts. Future research can aim to further build upon this paper by examining new leadership behaviors and contingency factors to make this leadership approach more targeted to the information security context.

Appendix A. Leadership Behaviors as presented by Northouse (2015)

Leadership Style	Description
Directive behavior	Makes sure tasks are clear and easy to understand
Supportive behavior	Attempts to ensure a friendly and approachable relationships that supports fair treatment
Participative behavior	Attempts to involve subordinates in decision making to produce better outcomes
Achievement-oriented behavior	Challenges subordinates to produce the best possible outcome

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, *39*, 396-405.

Boss, S R, Kirsch, L J, Angermeier, I, Shingler, R.A., & Boss, R.W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

Bradbury, D. (2011). A Day in the Life of a CISO. *Infosecurity*, *8*(3), 24-27.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*(3), 18-41.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, *19*(4), 391-412.

Dunkerley, K., & Tejay, G. (2009). Developing an information systems security success model for egovernment context. *AMCIS 2009 Proceedings*, 346.

Elahi, G., & Yu, E. (2007). A goal oriented approach for modeling and analyzing security trade-offs. In *Conceptual Modeling-ER 2007* (pp. 375-390). Springer Berlin Heidelberg.

Evans, M. G. (1970). The effects of supervisory behavior on the path-goal relationship. *Organizational Behavior and Human Performance*, *5*(3), 277-298.

Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security*, *16*(5), 257-263.

Groysberg, B., Kelly, L. K., & MacDonald, B. (2011). The new path to the C-suite. *Harvard Business Review*, *89*(3), 60-68.

Hardekopf, B. (2015). Data breaches of 2014. *Forbes.* Retrieved from http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Holloway, J. B. (2012). Leadership Behavior and organizational climate: An empirical study in a non-profit organization. *Emerging Leadership Journeys*, *5*(1), 9-35.

House, R. J. (1971). A path goal theory of leader effectiveness. *Administrative Science Quarterly*, 321-339.
House, R. J., & Mitchell, R. R. (1974). Path-goal theory of leadership. *Journal of Contemporary Business*, 3, 81-97.
House, R. J., & Mitchell, T. R. (1975). *Path-goal theory of leadership* (No. TR-75-67). Washington University, Seattle: Department of Psychology.
House, R. J. (1996). Path-goal theory of leadership: Lessons, legacy, and a reformulated theory. *The Leadership Quarterly*, *7*(3), 323-352.
Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.
Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, (3), 16-24.
Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126-129.
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, *34*(3), 549-566.
Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134.
Keller, R. T. (1989). A test of the path-goal theory of leadership with need for clarity as a moderator in research and development organizations. *Journal of Applied Psychology*, *74*(2), 208.
Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help. *Network Security*, *1*, 327.
Koskosas, I. V., & Asimopoulos, N. (2011). Information System Security Goals. *International Journal of Advanced Science and Technology*, *27*, 15-26.
Li, Y., Tan, C. H., & Teo, H. H. (2012). Leadership characteristics and developers' motivation in open source software development. *Information & Management*, *49*(5), 257-267.
Malik, S. H., Aziz, S., & Hassan, H. (2014). Leadership Behavior and Acceptance of Leaders by Subordinates: Application of Path Goal Theory in Telecom Sector. *International Journal of Trade, Economics and Finance*, *5*(2), 170-175.
Momeni, N. (2009). The relation between managers' emotional intelligence and the organizational climate they create. *Public Personnel Management*, *38*(2), 35-48.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.
Northouse, P. G. (2015). *Leadership: Theory and Practice*. Sage publications.
Oladimeji, E. A., Supakkul, S., & Chung, L. (2006). Security threat modeling and analysis: A goal-oriented approach. In *Proceedings of the 10th IASTED International Conference on Software Engineering and Applications*, pp. 13-15, November, 2006.
Perlroth, N. (2014). A tough corporate job asks one question: Can you hack it?. *New York Times.* Retrieved from http://www.nytimes.com/2014/07/21/business/a-tough-corporate-job-asks-one-question-can-you-hack-it.html, July 20, 2014.
Sagie, A., & Koslowsky, M. (1994). Organizational attitudes and behaviors as a function of participation in strategic and tactical change decisions: an application of path–goal theory. *Journal of Organizational Behavior*, *15*(1), 37-47.

Schriesheim, C. A., & DeNisi, A. S. (1981). Task dimensions as moderators of the effects of instrumental leadership: A two-sample replicated test of path–goal leadership theory. *Journal of Applied Psychology*, *66*(5), 589.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296-302.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198.

Vecchio, R. P., Justin, J. E., & Pearce, C. L. (2008). The utility of transactional and transformational leadership for predicting performance and satisfaction within a path-goal theory framework. *Journal of Occupational and Organizational Psychology*, *81*(1), 71-82.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215-218.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Von Solms, R., & Von Solms, S. B. (2006). Information security governance: Due care. *Computers & Security*, *25*(7), 494-497.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198.

Weathersby, G. B. (1999). Leadership vs. management. *Management Review*, *88*(3), 5.

Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems*, *48*(3), 15.