# Archetypes to Inform Information Security: The Organization Man and the Innovator

*Research-in-Progress*

**Rahul Singh**
University of North Carolina at Greensboro
rahul@uncg.edu

**Jeffrey D. Wall**
University of North Carolina at Greensboro
jdwall2@uncg.edu

**Gurpreet Dhillon**
Virginia Commonwealth University
gdhillon@vcu.edu

## Abstract

Prevalent organizational structures used to deter security deviance may limit organizational action to mitigate threats, particularly if the threats are novel. We contrast two archetypal personae: the Organization Man (Whyte 1956) and the Innovator (Levi-Strauss 1966) to understand behavior in security-sensitive situations to provide a novel direction for information security research. This paper develops a theoretical foundation to posit that both the Organization Man and the Innovator are necessary for secure Information Systems. Moreover, they serve unique and disjoint perspectives to develop new understanding of employee behavior regarding information security in organizations. Understanding the characteristics of these archetypal personae in security-related situations can improve our current understanding of individuals' security-related behaviors in organizations.

### Keywords (Required)

Information security, security threat, Organization Man, the Innovator.

## Introduction

Information system (IS) security issues are costly to organizations. The Computer Security Institute (CSI) reports that, on average, organizations lose more than $200,000 annually to security breaches (Richardson 2009; Richardson 2011). Thus, preventing and responding to security breaches is a crucial endeavor in the workplace. Behavioral information security research explains why employees engage in deviant security-related acts, how to deter these deviant behaviors, and how employees can be used as security assets. However, the role of employees and their behavior regarding information security in organizations remains an active and unsettled area of research. Some security studies suggest employees may be a major cause for security problems (Warkentin and Willison 2009; Workman and Gathegi 2007). However, studies also suggest that employees can be great security assets (Bulgurcu et al. 2010). Thus, there is some ambiguity in the guidance that research provides regarding employee behaviors and their impact on information security in an organization. This motivates the need for different theoretical perspectives to inform and guide security research regarding employee behavior and behavioral impacts on information security in organizations.

This research attempts to develop an understanding of employees' security-related behaviors by studying how well-studied archetypal personae explain security behavior. Despite multiple research studies on organizational security and employee behavior, information security research has adopted few guiding archetypes (Rosenfeld et al. 2007). Archetypes are useful in guiding research in academic disciplines (Xue et al. 2008). We argue that the prevalent prescriptive organizational structures for deterring security-related deviance in employees may limit organizational action to mitigate threats, particularly with regard to novel and emergent security threats. Specifically, we contrast two archetypal personae: the Organization Man (Whyte 1956) and the Innovator—the Bricoleur and Engineer (Levi-Strauss 1966). Archetypes tend to be broad, general, and encompassing; therefore, models that rely on the archetypes in this paper may result in more parsimonious models. Although archetypes may not capture nuance, they do represent general patterns in a simple manner. The archetypes presented in this paper provide a basis to understand individuals' behavior in security-sensitive organizational situations and provide a foundation for future security research.

This paper develops novel theoretical foundations to posit that both the Organization Man and the Innovator are necessary to ensure secure IS. Moreover, they serve unique and disjoint perspectives to develop new understanding of employee behavior regarding information security in organizations. However, organizations are established to support the Organization Man. Thus, the Innovator may be viewed as deviant or a threat. We seek to alter these perceptions by identifying the important role the Innovator plays in information security settings. Understanding the characteristics of these archetypal personae in security-related situations can improve our current understanding of individuals' security-related behaviors in organizations. This paper proposes a series of security-related propositions to develop deep understanding about the role of these archetypes in organizations and better understand the implications of our theoretical contribution. In addition, we describe our on-going case-based approach and discuss how this informs new avenues of investigation for individuals' information security related behaviors in organizations.

The remainder of this paper is organized as follows. First, an understanding of the Organization Man and the Innovator archetypes are offered. Second, a discussion of the ability of the Organization Man and the Innovator to comply with security policy, identify security vulnerabilities, and respond to security breaches is given. Third, a research design is proposed to test the assertions made in this paper. Lastly, implications for using the archetypes presented in this paper are shared.

## Background

Conceptually, we develop the characteristics of the Organization Man and the Innovator in relation to compliance with security policies, identification of security vulnerabilities in Information Systems, and development of responses to security breaches. The Organizational Man and Innovator archetypes offer contrasting approaches and positions to these pervasive organizational information security issues. Moreover, an understanding of these archetypes and subsequent consideration of organizational information security issues from the perspectives of these archetypes sensitize new ways of seeing (Burke 1965). We develop these analytic perspectives to provide theoretically informed bases for novel conceptualizations, analysis and interpretations.

### *The Organization Man*

The Organization Man is a follower and essential driving force of the modern organization (Whyte 1956). The Organization Man is bound by the Social Ethic created to sustain the modern organization. Importantly, scientism is a foundational principle of the Social Ethic. Whyte (1956) describes scientism in the Social Ethic as the pursuit of the "science of man." The goal of scientism in the Social Ethic is to find ways to conform the behaviors of the Organization Man to the goals of the organization. Whyte (1956) suggests that educational institutions, governments, communities, and organizations themselves help to reify the role of the Organization Man.

The actions of the Organization Man are constrained by organizational structures, work routines, and policies created to maintain the Social Ethic. Examples of these constraints include organizational hierarchies, protocols, and policies. These bureaucratic controls are currently the culturally dominant form of organizational control (Cardinal, 2001) and security-related governance. Subscribing to the Social Ethic, the Organization Man submits to working within the bounds of these constraints, sometimes unknowingly. Importantly, the Innovator, particularly the Engineer, may be the source of the controls by which the Organization Man is bound (French, 1967). Organizations are established to encourage the loyalty and compliance of the Organization Man.

### *The Innovator*

As considered here, the Innovator is an amalgam of two archetypes described by Levi-Strauss (1966)—the Engineer and the Bricoleur. While they are both innovators, the Engineer and the Bricoleur rely on different means to achieve innovation. The Engineer uses the scientific method to create innovative artifacts. The Bricoleur, on the other hand, generates innovation by combining available resources to create new resources in an ad-hoc manner. The Engineer, therefore, considers resources beyond their immediate reach to create something novel, while the Bricoleur is bound by his immediate environment (Levi-Strauss 1966). Importantly, the Innovator tends to think of the greater good based on individual and social contributions, making the Innovator less reliant on organizational structure and policy (French 1967).

Levi-Strauss (1966) refers to the Bricoleur's methods of generating knowledge and innovation as a "savage" mindset. However, he does not suggest that the Bricoleur's methods are inferior to the Engineer's. He claims that the term "savage mind" is arbitrary and useful only to present the dichotomy between the Engineer and Bricoleur. Both the methods of the Bricoleur and Engineer have strengths and weaknesses. For example, the mindset of the Bricoleur is useful in emergency situations where ad hoc, resourceful thinking is required to handle the novelty and uncertainty of emergent conditions (Kroll-Smith et al. 2007). The Engineer's mindset, on the other hand, is useful for establishing reliability and predictability. Similarly, the Engineer's process is far more considerate, and therefore, less efficient. The Bricoleur's process, however, is resourceful and adaptable, making it more efficient. We consider an amalgam of these archetypes since we focus on the innovative output, not considering for the time being, the method by which the innovation is achieved.

## Conceptual Development

### *Organizational Strain and Archetypal Adoption*

The Organization Man and the Innovator are not static organizational agents. Instead the Organization Man and the Innovator represent personae that employees may assume at different times as needed by the organizational situation. However, this paper also acknowledges that employees are likely to adopt a more permanent persona based on personal traits, roles, and external pressures. For example, employees with high levels of commitment are more likely to adopt the persona of the Organization Man (Randall 1987). Similarly, because of work roles, managers tend to assume the persona of the Organization Man, while employees in research and development positions tend to adopt a persona more like the Innovator (French 1967). In general, organizational structure, pressures to work efficiently, and other normative pressures lead most employees to adopt a persona more like the Organization Man (DiMaggio and Powell 1983; Randall 1987).

Further, organizational actions are guided by an *aspiration level* — an expected level of organizational performance (Cyert and March 1963). In normal operating conditions, employees tend to follow a routine and are more risk averse (Kahneman and Tversky 1979; March 1997). Routine and controllability are important values in the Social Ethic, as they help to control the Organization Man. Therefore, when organizations are under little or no duress, employees are more likely to allow structures, roles, and norms to guide their actions.

Merton's (1938) strain theory suggests that individuals unable to attain societally desirable goals through legitimate means may seek to attain the goals through non-routine means. The Innovator often tends to be stifled by organizational structure and policy and seems more likely to emerge when an organization experiences strain. When organizations experience strain that causes performance to drop below aspirations and expectations, employees may be less risk averse and more likely to seek alternative ways of thinking or acting to restore performance to aspired levels (Lehman and Ramanujam 2009; March 1991). This tendency towards alternative innovative thinking is reflected in the Innovator, particularly the Bricoleur. The Bricoleur thrives in emergent, strenuous conditions (Kroll-Smith et al. 2007). It is reasonable that when faced with significant and novel security threats, organizational performance is below its aspiration level. In summary, we propose:

> *Proposition 1a: Under normal operating conditions, employees will be more likely to assume the persona of the Organization Man than the Innovator.*
>
> *Proposition 1b: Under the threat of large, novel security threats, employees will be more likely to assume the persona of the Innovator than under normal operating conditions.*

It is important to note that Proposition 1b does not imply that the Innovator will be the dominant persona under strenuous conditions. Organizational structures and external regulation may discourage alternative thinking, even when organizations are strained (Lehman and Ramanujam 2009). Thus, the Organization Man may be the dominant mindset under all conditions.

## *Complying with Security Policy*

The Organization Man is dedicated to policy and protocol. SETA programs (Security education training and awareness) are commonly used to influence security-related behaviors of employees. Organizational and social structures pressure employees to adopt the persona of the Organization Man (Whyte 1956). While the Organization Man is a policy follower, the Innovator looks beyond extant policy, protocol, and structure, perhaps to create new policy (French 1967). Therefore, the Innovator may be less likely to comply with policy than the Organization Man. The Innovator seeks novel and better ways of operating. Thus, the Innovator may view policy as an impediment to progress, and be more likely to ignore policy to pursue better operating procedures. Still, the Innovator is likely to receive greater pressure to comply with policy under normal organizational conditions than in emergent conditions. Under normal conditions, the Innovator is more likely to assume the persona of the methodic, process oriented Engineer than that of the Bricoleur.

Organizational strain creates an environment suited for the Innovator, particularly for the Bricoleur. The Bricoleur thrives in emergent, strenuous conditions (Kroll-Smith et al. 2007). In emergencies, the resourcefulness of the Bricoleur is useful for handling difficult situations. However, under duress, the persona of the Bricoleur may disregard norms, policies, or even laws (Kroll-Smith et al. 2007). Thus, we propose the following propositions:

> *Proposition 2a: Under normal operating conditions, the Innovator will be less likely to comply with security policy than the Organization Man.*
>
> *Proposition 2b: Under the threat of large, novel security problems, the gap in policy compliance between the Organization Man and the Innovator will be greater than the gap under normal conditions.*

Figure 1 presents the gap in compliance that may exist between the Innovator and the Organization Man under normal and strenuous conditions.

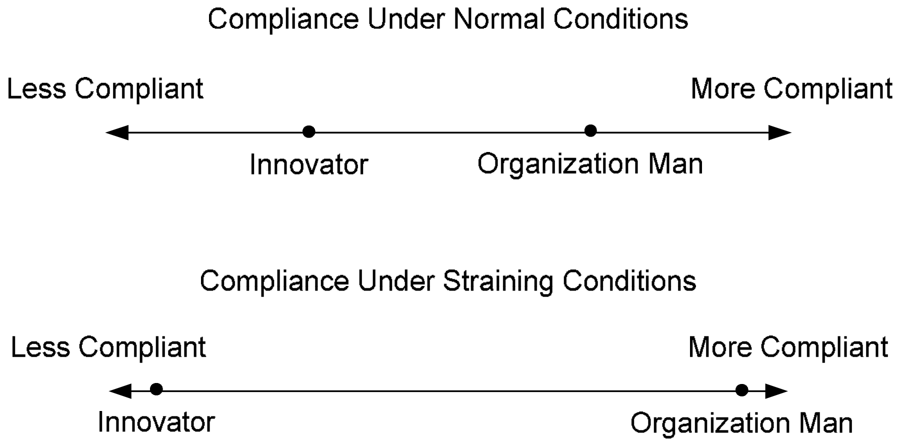

**Figure 1. Likelihood of Policy Compliance under normal and straining conditions**

## *Identifying Security Vulnerabilities*

The Innovator is an experimenter and tinkerer. In methodically testing IS or tinkering with new ways of using IS in the absence of a security breach, the Innovator may advertently or inadvertently discover security vulnerabilities. For example, security professionals often intentionally test vulnerabilities in organizational information systems in new ways to discover unknown weaknesses. Others in the organization who adopt the persona of the Innovator may also be very useful in discovering security vulnerabilities. Employees who tinker with systems in novel ways may inadvertently discover vulnerabilities that lead to more secure IS. The Organization Man, on the other hand, is likely to use IS only as suggested by policy and for routine purposes, and therefore, less likely to find security vulnerabilities in the organizational information systems.

The Organization Man is a follower of routine, and is very likely to notice deviations in procedure. Security breaches that disrupt routine procedures are likely to be noticed quickly by an employee following the Organization Man archetype. For example, an accountant following daily routine is likely to identify a discrepancy between recorded and actual cash flows in sales caused by a security breach. Similarly, a security professional could identify unwanted traffic in an IS through routine system monitoring. The Innovator, however, is not tied to routine. Always tinkering or experimenting, the Innovator is less likely to notice deviations from routine since there is no consistent routine to disrupt. Thus, we propose:

> *Proposition 3a: In the absence of a security breach, the Innovator will be more likely to identify security vulnerabilities in an IS than the Organization Man.*
>
> *Proposition 3b: In the presence of a security breach, the Organization Man will be more likely to identify security vulnerabilities in an IS than the Innovator.*

Figure 2 presents reversal that occurs in the ability of the Organization Man and the Innovator to identify security vulnerabilities under different breach conditions.

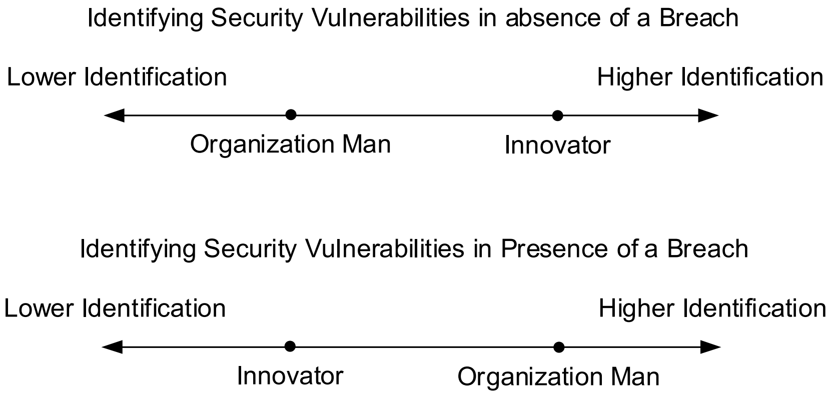

**Figure 2. Likelihood of identifying security vulnerabilities under breach and non-breach conditions**

### *Responding to Security Breaches*

Organizations develop Incident Response Plans (IRP) to prepare for security breaches. An IRP describes known security threats, people to contact if the breach occurs, as well as procedures that constitute appropriate response to the breach (Staggs 2009). This formulaic plan is useful for guiding the actions of the Organization Man. When a known breach occurs, the Organization Man is likely to follow protocol prescribed by the IRP to resolve the security issue. Therefore, the Organization Man will respond quickly to known security threats to the extent that the organization has developed an effective IRP and has adequately trained employees to use it. The Innovator, however, may be more likely to ignore policy and protocol to find an alternate solution. Solutions developed by the Innovator may require more time and effort to develop than rote responses. Similarly, any response developed by the Innovator in a short period of time could result in failure or be less effective than planned responses.

The persona of the Innovator thrives in emergent situations, while the persona of the Organization Man relies on procedure to respond to situations, including novel situations. The Organization Man, therefore, is unlikely to respond well to novel security threats. Controls and governance mechanisms, such as IRPs, exist for known threats. Unfortunately, just as technology is ever evolving, so are IS security threats. Procedures cannot be created for a breach until an organization has experienced it, or otherwise considers it. The Innovator, particularly the Bricoleur, is responsive and reactive to novel situations. The Innovator could, therefore, devise novel responses more quickly. Although the solutions are not guaranteed to work, the response of the Innovator may be more effective than no response. Thus, we propose:

> *Proposition 4a: Under the threat of a familiar security breach covered by an existing Incident Response Plan, the Organization Man is more likely to respond quickly and suitably to the threat than the Innovator.*
>
> *Proposition 4b: Under the threat of a large, novel security breach, the Innovator is better equipped to respond more quickly and suitably to the threat than the Organization Man.*

Figure 3 presents reversal that occurs in the ability of the Organization Man and the Innovator to respond to security threats under different breach conditions.

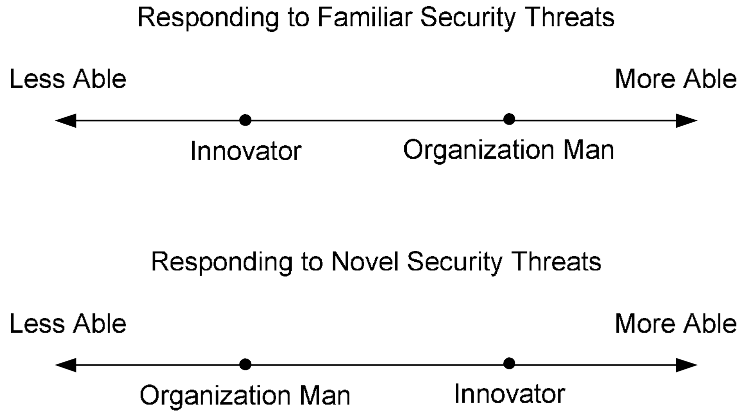

**Figure 3. Ability to respond to familiar and novel security threats**

## Research Design and Case Study

The archetypes described in this paper are novel considerations in security research. Thus, research has not validated their existence in the security context. In this section, we introduce The Tower as an organizational case context to describe the manifestation and importance of the archetypes of the Organization Man and the Innovator using the propositions we have developed. The case study was conducted over a 12 month period when structural changes were being implemented at the case organization. All interviews were recorded and undertaken in the tradition of Waltham's (1993) interpretive research design. Space limitations forbid us from presenting the pros and cons of case study work. Interpretive research designs are however well accepted in the literature and we strictly followed the tenants in conducting the case study.

### *The Tower – An Illustrative Case*

The Tower is a major hotel and casino property located in a thriving tourist location in the US. Security is an important aspect to ensure smooth operations. Security at the Tower is provided by two departments, Gaming Surveillance and General Physical Security, each with its own management. Management in security has been in place since a 1995 expansion and change of ownership.

#### Strain at the Tower

Since the expansion, the IT manager has often stated that he feels the present security management is ineffective and they should not be an independent department. Security management has felt that IT has interfered with the operation and confidentiality of security investigations. Security Officers felt unnerved when, while they were working on a report, IT personnel would take control of the screen. IT would explain that they were correcting problems and needed to test the system. Similar strains between the departments at the organization reveal different archetypal behaviors under normal and strained conditions.

### Compliance at the tower

The Security department found itself becoming more and more reliant on Information Technology. The CFO set up a committee to investigate compliance in the organization, chaired by the IT Director and with representation from each department in the organization. Department representatives reported lower levels of compliance, which steadily improved. The increased focus on compliance placed restrictions on acquisition and installations of hardware and software in the organization. On the surface this appeared to be a logical procedure. However, interestingly, this created additional tensions in the organization.

### Identifying Vulnerabilities at the Tower

Since the discovery of several viruses on the network, the IT department decided to throw the proverbial baby out with the bath water. Instead of implementing competent malware prevention, they decided to take the drives out of all network computers. The conceptual model that was held by the Security Department was not the same one seen by IT. These needed to be brought together.  Ultimately, the mistrust of IT for anyone outside their department led them to remove drives from all the computers on the network.

### Responding to Security Breaches at the tower

The organization implemented a new dispatch system, which took nearly 2 years to become operational. Some dispatchers learned several tricks to keep the program up and running. These dispatchers adopted out of system behaviors, which may cause security breaches in the long run. Several other dispatchers asked for changes of assignment or left the company rather than keep fighting to comply with a faulty program. The report-writing module that was going to provide a link among the Officers on the floor, Risk Management, and Investigations still gathers dust in the Manager's office. The only people who bothered to learn how it worked, have left the company.

## Discussion

This paper has identified two archetypes—the Organization Man and the Innovator—to inform future IS security research. This paper has suggested that the two archetypal personae react to security situations differently. However, the modern organization is structured in a way that primarily encourages the adoption of the Organization Man persona and mostly discourages the participation of the Innovator. Yet the Innovator has much to add to organizational security. What may appear to be noncompliant behavior may be novel approaches to addressing security issues under limited resources. The Organization Man is not highly responsive. Thus, it may be in the best interest of organizations to accommodate multiple personae.

Given that the Innovator is discouraged from acting in organizations, this paper suggests that organizations should seek to establish structures that allow both the Organization Man and the Innovator to thrive. A structure and policies that encourage employees to adopt the persona of the Organization Man in normal conditions and the persona of the Innovator in emergent conditions could benefit the organization by relying on the strengths of each persona.

Organizations that encourage employees to adopt the persona of the Innovator, particularly that of the Bricoleur, need to encourage strong ethical guidelines. The Bricoleur tends to disregard policies, rules, and norms (Kroll-Smith et al. 2007), particularly in straining situations (Lehman and Ramanujam 2009). Therefore, certain values may need to be deeply rooted in employees to avoid unethical or illegal actions.

These propositions are grounded in strong theoretical foundations that are novel in their application to information systems security literature. We have developed the conceptualizations based on strong theory and grounded them in our case study to develop propositions that lead to theorizing about information security behaviors under a variety of security conditions.

## Conclusions

This paper has presented a series of propositions to be tested. This paper, being a work in progress, will seek to test these propositions as discussed above. Since these archetypes have never been examined in a security setting, researchers should be reluctant to use them before they are tested.

Archetypes are useful for guiding research in a given field (Xue et al. 2008). The archetypes described in this paper should act as a strong foundation for future security research. For example, future research might consider how the Organization Man and the Innovator respond to social engineering attacks. It may be that the Organization Man is more susceptible to social engineering because social engineers use existing social and organization structures to take advantage of victims. Since the Organization Man is more likely to adhere to social and organizational norms and structure, those who adopt the persona of the Organization Man may be more vulnerable.

Similarly, the rigid policies and protocols created by the Social Ethic may lead the Organization Man to consider only the procedural aspects of security. The mindset of the Organization Man, therefore, may focus on rote compliance, but ignore the overall goal of making IS more secure. It could be that the Innovator is more focused on the end goal, which could lead to more secure IS.

## REFERENCES

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Cardinal, L.B. 2001. "Technological Innovation in the Pharmaceutical Industry: The Use of Organizational Control in Managing Research and Development," *Organization Science* (12), pp. 19-36.

Cyert, R., and March, J.G. 1963. *A Behavioral Theory of the Firm*. Englewood Cliffs, NJ: Prentice Hall.

DiMaggio, P., and Powell, W.W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* (48:2), pp. 147-160.

French, E.B. 1967. "The Organization Scientist: Myth or Reality," *Academy of Management Journal* (10:3), pp. 269-273.

Kahneman, D., and Tversky, A. 1979. "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* (47), pp. 263-291.

Kroll-Smith, S., Jenkins, P., and Baxter, V. 2007. "The Bricoleur and the Possibility of Rescue: First-Responders to the Floodin of New Orleans," *Journal of Public Management and Social Policy* (2007:Fall), pp. 5-21.

Lehman, D.W., and Ramanujam, R. 2009. "Selectivity in Organizational Rule Violations," *Academy of Management Review* (34:4), pp. 643-657.

Levi-Strauss, C. 1966. *The Savage Mind*. Chicago, IL: University of Chicago Press.

March, J.G. 1991. "Exploration and Exploitation in Organizational Learning," *Organization Science* (2), pp. 71-87.

March, J.G. 1997. "How Decisions Happen in Organizations," in *Organizational Decision Making,* Z. Shapira (ed.). New York, NY: Cambridge University Press, pp. 9-34.

Merton, R.K. 1938. "Social Structure and Anomie," *American Sociological Review* (3), pp. 672-682.

Randall, D.M. 1987. "Commitment and the Organization: The Organization Man Revisited," *Academy of Management Review* (12:3), pp. 460-471.

Richardson, R. 2009. "14th Annual Csi Computer Crime and Security Survey," Computer Security Institute, pp. 1-14.

Richardson, R. 2011. "15th Annual 2010/2011 Computer Crime and Security Survey," Computer Security Institute, pp. 1-44.

Rosenfeld, S.N., Rus, I., and Cukier, M. 2007. "Archetypal Behavior in Computer Security," *Journal of Systems and Software* (80:10), pp. 1594-1606.

Staggs, K. 2009. "Build a Cyber Security Incident Response Plan," *Control Engineering* (56:12), p. 56.

Walsham, G. (1993). *Interpreting information systems in organizations*. Chichester: John Wiley & Sons.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18), pp. 101-105.

Whyte, W.H. 1956. *The Organization Man*. Garden City, NY: Doubleday.

Workman, M., and Gathegi, J. 2007. "Punishment and Ethics Deterrents: A Study of Insider Security Contravention," *Journal of the American Society for Information Science and Technology* (58:2), pp. 212-222.

Xue, Y., Liang, H., and Boulton, W.R. 2008. "Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context," *MIS Quarterly* (32:1), pp. 67-96.