

Volume 3, Number 2

ISSN 2150-5136

**Allied Academies
International Conference**

**Las Vegas, Nevada
October 12-15, 2011**

**Academy for
Studies in Business**

PROCEEDINGS

Copyright 2011 by the DreamCatchers Group, LLC, Arden, NC, USA

All authors execute a publication permission agreement taking sole responsibility for the information in the manuscript. The DreamCatchers Group, LLC is not responsible for the content of any individual manuscripts. Any omissions or errors are the sole responsibility of the individual authors.

The Academy for Studies in Business Proceedings is owned and published by the DreamCatchers Group, LLC, PO Box 1708, Arden, NC 28704, U.S.A., (828) 507-9770. Those interested in the *Proceedings*, or communicating with the *Proceedings*, should contact the Executive Director of the Allied Academies at info@alliedacademies.org.

Copyright 2011 by the DreamCatchers Group, LLC, Arden, NC

Table of Contents

THE DODD-FRANK ACT AND WHISTLEBLOWER PROTECTION..... 1
 Gerald E. Calvasina, Southern Utah University
 Richard V. Calvasina, University of West Florida
 Eugene J. Calvasina, Southern University

EXAMINING MOTIVATION THEORY IN HIGHER EDUCATION: PRODUCTIVITY OF TENURED FACULTY 5
 Brent C. Estes, Sam Houston State University
 Barbara Polnick, Sam Houston State University
 Ryan K. Zapalac, Sam Houston State University

SERVANT LEADERSHIP’S IMPACT ON PROFIT, EMPLOYEE SATISFACTION, AND EMPOWERMENT WITHIN THE FRAMEWORK OF A PARTICIPATIVE CULTURE IN BUSINESS 9
 David Jones, Southern Wesleyan University

GOING WHERE ANGELS FEAR TO TREAD: AUCTIONING UNIVERSITY PARKING TO ENHANCE REVENUE 13
 Michael A. McCollough, University of Idaho
 Steven R. Shook, University of Idaho

THE BIGGEST THREAT TO THE U.S. DIGITAL INFRASTRUCTURE: THE CYBER SECURITY WORKFORCE SUPPLY CHAIN..... 15
 Aleta Wilson, University of Maryland University College
 Amjad Ali, University of Maryland University College

THE DODD-FRANK ACT AND WHISTLEBLOWER PROTECTION

Gerald E. Calvasina, Southern Utah University
Richard V. Calvasina, University of West Florida
Eugene J. Calvasina, Southern University

ABSTRACT

The enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act P.L. 111-203 (Dodd-Frank Act) in July of 2010 added yet another piece of federal regulation designed to protect “whistleblowers”. While the plethora of regulation at the federal and state levels designed to protect whistleblowers continues to grow, there is scant evidence that the regulatory initiatives have had a significant effect on protecting whistleblowers, corporate fraud, and government waste. The purpose of this paper is to examine federal regulation designed to protect whistleblowers focusing on the most recent efforts, the Patient Protection and Affordable Care Act of 2010 (Affordable Care Act) and the Dodd-Frank Act.

BACKGROUND

There are 21 federal statutes enforced by the United States Occupational Safety and Health Administration (OSHA), and accompanying regulations designed to protect whistleblowers. While most of the attention regarding whistleblower rights in recent years has been directed at perceived problems in the financial services sector of the U.S. economy, the primary focus at the federal level has always been on protecting whistleblower rights with respect to safety and health in the workplace. Over time, everything from commercial motor carrier safety to corporate fraud and Security and Exchange Commission (SEC) rules and regulations have come under the OSHA umbrella of protections afforded to whistleblowers. Allen Smith notes that the emphasis away from safety and health issues “began in earnest with the enactment of SOX (Sarbanes-Oxley) in 2002 and continued with the Consumer Product Safety Act in 2008, American Recovery and Reinvestment Act of 2009 and the Fraud Enforcement and Recovery Act in 2009” (Smith, 2010). Following these, Congress enacted the Patient Protection and Affordable Care Act of 2009 P.L. 111-148 (Affordable Care Act) and the Dodd-Frank Act (2010) which also added whistleblower protection for employees under the OSHA umbrella.

Recent reports present a mixed perspective as to the effectiveness of federal regulation regarding the protection of whistleblowers. In 2003, Ron Hayes then a member of the National Advisory Committee on Occupational Safety and Health (NACOSH) charged that OSHA had a “dismal record” of protecting whistleblowers and pointed to the declining number of complaints being filed with the agency as evidence that workers’ confidence in OSHA’s ability to protect them was waning (Nash, 2003). Other concerns voiced included the increased responsibility that Congress was giving to OSHA to enforce whistleblower protection in areas beyond safety and

health. In 2003 it was Sarbanes-Oxley (Nash, 2003). Another report by a “watchdog group” Public Employees for Environmental Responsibility (PEER), claims “that OSHA does not effectively protect workers who report health and safety hazards” (safety.blr.com, 2011). According to PEER Executive Director Jeff Ruch, “the problem of ineffective protection is compounded by a culture of reprisals within OSHA against its own specialists who voice concerns about agency deficiencies” characterizing this culture as being a “notorious weakness of the OSHA whistleblower program” (safety.blr.com, 2011). The PEER group cited the case of Robert Whitmore, a former OSHA employee who the group alleges was “unfairly dismissed in 2009 for criticizing OSHA’s performance with respect to protecting whistleblowers (safety.blr.com, 2011).

AFFORDABLE CARE ACT PROTECTIONS

Public law 111-148, the Affordable Care Act, amended section 1558 of the Fair Labor Standards Act by adding Section 18C “Protections for Employees”. Section 18C prohibits employers from discharging or discriminating against any employee regarding their whistleblower rights and outlines specific protections for employees.

DODD-FRANK ACT

Section 922 of Dodd-Frank contains the latest in whistleblower protection requirements designed to protect employees. In addition to providing monetary incentives for whistleblowers to provide information to federal authorities, the requirements “strengthen the whistleblower protection provisions of the Sarbanes-Oxley Act and the False Claims Act, and create additional whistleblower retaliation causes of action” (Oswald and Zuckerman, 2011). The act also establishes a whistleblower program that enables the Securities and Exchange Commission (SEC) to pay awards under regulations prescribed by the SEC and subject to certain limitations to eligible whistleblowers (SEC, 2011). These awards will be paid out of a statutorily-created Investor Protection Fund that as of this writing has a balance in excess of \$450 million (SEC, 2011). Individuals may file anonymous complaints but, to be considered for financial awards under the program those who want to remain anonymous must submit their information through an attorney. The act also prohibits retaliation by employers against individuals who become whistleblowers under the SEC rules even if they do not recover a whistleblower award. A private cause of action is also available to individuals if they are discharged or discriminated against by their employers under the act (SEC, 2011).

These aspects of the Dodd-Frank Act are not without their critics. With respect to the financial incentives provisions, some observers have predicted that the act and the ensuing SEC regulations will lead to increases in whistle-blower payouts and in turn motivate employees to by-pass internal complaint procedures that companies may have in place (Smith, 2011 A). Steven Pearlman, an attorney with Seyfarth Shaw in Chicago, said that “the bounty provisions give whistle-blowers a frightening incentive to let financial improprieties grow so that the size of the SEC’s recovery and their corresponding bounty is higher” (Smith, 2011, B). The SEC

approved its rule on this issue on May 25, 2011 and the rule does “permit whistle-blowers to go directly to the SEC for a bounty for their tips without first using a company’s internal compliance program” (Smith, 2011 B).

The final SEC rules specify that “any individual who provides the SEC with information that relates to a possible violation of the federal securities laws can qualify as a whistle-blower” (Lawrence-Hardy and Peifer, 2011). Four basic requirements for an award are noted:

The whistle-blower has to “voluntarily” provide the SEC with information relevant to a possible securities violation.

The whistle-blower’s information must be “original.

The information has to lead to a successful SEC enforcement action.

The enforcement action has to result in monetary sanctions, including penalties and interest that exceed \$1 million (Lawrence-Hardy and Peifer, 2011).

According to Lawrence-Hardy and Peifer, the Dodd-Frank Act’s anti-retaliation provisions “dramatically expand the anti-retaliation protection for employees who report potential securities violations” and that “the SEC’s final rules make clear that those protections apply regardless of whether a whistle-blower qualifies for an award under the new bounty program” (Lawrence-Hardy and Peifer, 2011 Source: H.R. 4173). Additionally, the Dodd-Frank Act significantly broadens the statute of limitations with respect to the anti-retaliation protection. While initially, the statute increased the time an individual has to file a complaint with OSHA under SOX from 90 to 180 days, “employers who discipline, threaten, or otherwise discriminate against employees for whistle-blowing activities may be sued directly in federal court up to 10 years after the retaliation occurs”(Lawrence-Hardy and Peifer, 2011). Individuals are also entitled to jury trials and “employees who prevail in a retaliation action are entitled to reinstatement, double back-pay with interest and the litigation expenses that they incur pursuing that relief” (Lawrence-Hardy and Peifer, 2011).

HOW SHOULD EMPLOYERS PREPARE

The literature is clear at this time, that employers will need to enhance their internal compliance efforts to facilitate compliance with the whistle-blower protections contained in recent congressional action and SEC rules. One consistent recommendation has been to focus on efforts to “create a culture of integrity” (Smith, 2011, B). In reality, this recommendation is often very much easier said than done. Popular clichés in the literature include “positive employee relations”, a focus on “top-down efforts at creating transparency and accountability”, and communication efforts designed to enhance “a commitment to ethics to employees of all levels” (Meinert, 2011 and Smith, 2011, B). Training and education on how internal compliance systems, including anonymous hotlines, employee surveys, and complaint processes are supposed to work, is also a consistent theme (Lawrence-Hardy and Peifer, 2011, Smith 2011, B, and Petrulakis and Parsons, 2011). Employers should enhance efforts to make sure all employees understand how systems are supposed to work. This is especially true for lower level supervisors who are very often the first members of management to be made aware of concerns that

employees may have. Additionally, if organizations are serious about creating a culture of integrity, codes of conduct, ethical standards, and clear anti-retaliation policies are key elements associated with these efforts.

Whatever system is developed, the system should be easy to utilize for employees and provide for as much protection for confidentiality as possible. When concerns are brought to managements' attention, prompt investigation is critical as well as feedback to individuals as to what the investigation uncovered and how the problems or issues were resolved (Meinert, 2011). Feedback to individuals and periodic posting of the results of investigations on company websites or in company publications have also been advanced as ways to demonstrate the organizations' commitment to creating a culture of integrity and trust (Meinert, 2011).

REFERENCES

- Affordable Care Act, 2010. Patient Protection and Affordable Care Act Health-Related Portions of the Health Care and Education Reconciliation Act of 2010, retrieved, 8/1/2011, from <http://docs.house.gov/energycommerce/ppacacon.pdf>.
- DOL, (2011). The Whistle Blower Protection Program, retrieved, 7/28/2011 from <http://www.whistleblowers.gov/index.html>.
- H.R. 4173, (2010). The Dodd-Frank Act. Retrieved 8/3/ 2011 from <http://www.sec.gov/about/laws/wallstreetreform-cpa.pdf#page=470>.
- Lawrence-Hardy, Allegra J and Peifer, Lee A. (2011). SEC's whistle-blower rules effective soon: what employers need to know now. Retrieved 8/2/2011 from <http://www.shrm.org/LegalIssues/EmploymentLawAreas/Pages/SECWhistleBlowerRules.aspx>.
- Meinert, Dori (2011). Whistle-blowers: threat or asset?, HRMagazine, Volume 56, Number 4, pp. 26-32.
- Nash, James (2003). Does OSHA protect health and safety whistleblowers?, EHSToday, retrieved 7/5/2011 from <http://www.printthis.clickability.com/pt/cpt?expire=&title=Does+O...>
- Oswald, R. Scott and Zuckerman, Jason (2011). Whistleblower provisions of the Dodd-Frank act. Retrieved 8/1/2011 from <http://www.employmentlawgroup.net/Articles/ROswald/DoddFrankWhistleblowerProvisions.html>.
- Petrulakis, Karen J. and Parsons, Alyssa Soares (2011). April 2011: new traps-whistle-blower protections in the Dodd-Frank act. Retrieved, 8/2/2011 from <http://www.shrm.org/Publications/LegalReport/Pages/NewTrapsWhistleBlowerProtections.aspx>.
- Safety.blr.com, (2011). Public employee group faults OSHA whistleblower protection, retrieved 7/5/2011 from <http://safety.blr.com/workplace-safety-news/safety-administration/OS...>
- SEC, (2011). U.S. Securities and Exchange Commission, Welcome to the office of the whistleblower website, retrieved 7/5/2011 from http://www.sec.gov/complaint/info_whistleblowers.shtml.
- Smith, Allen, (2010). Dodd-Frank act's expansive whistle-blowing protections continue trend. Retrieved 8/2/2011 from <http://www.shrm.org/LegalIssues/FederalResources/Pages/DoddFrankActWhistleBlowing.aspx>.
- Smith, Allen, (2011) A. Whistle-blowers' direct access to SEC questioned. Retrieved 8/2/2011 from <http://www.shrm.org/LegalIssues/FederalResources/Pages/DirectAccess.aspx>.
- Smith, Allen, (2011) B. SEC approves final whistle-blowing rule. Retrieved 8/3/2011 from <http://www.shrm.org/LegalIssues/FederalResources/Pages/SECWhistleBlowingRule.aspx>.
- Zuckerman, Jason (2010). Health care reform bill creates new whistleblower protections, retrieved from <http://www.todayworkplace.org/2010/03/26/health-care-reform-bill-creates-new-whistleblower-protections/>

EXAMINING MOTIVATION THEORY IN HIGHER EDUCATION: PRODUCTIVITY OF TENURED FACULTY

Brent C. Estes, Sam Houston State University
Barbara Polnick, Sam Houston State University
Ryan K. Zapalac, Sam Houston State University

ABSTRACT

In today's higher education landscape, universities and administrators are faced with a plethora of challenges. Perceived success for leaders and their respective institutions of higher learning are contingent on a myriad of issues ranging from recruitment and retention of students to comprehensive fiscal responsibility. Ultimately, though, like most organizations rely on the performance of their workers to determine success, one could argue that the success of a college or university is largely based on the productivity of its faculty. In that respect, higher education mirrors many organizations in today's business world in terms of its need to objectively evaluate the performance of its faculty.

Accurate assessment of faculty performance and productivity is an invaluable part of understanding, predicting, and influencing organizational success. Likewise, evaluation of faculty development in terms of skill, ability, and accomplishments is essential in determining an individual's value to his/her university. The knowledge and insight gained from these assessments allows these institutions of higher learning to become more efficient and ultimately more effective. Today, universities increasingly rely on such performance assessments to determine salaries and tenure rewards for their faculty members.

In most cases, however, performance and productivity cannot be measured objectively because there is no universal standard. Even among different departments within the same institution, there are often discrepancies with respect to defining productivity. What one department may value and consider productive, another department may regard as insufficient and lacking. According to Alchain and Demsetz (1962), this problem is a fundamental contributor to an organization's inability to accurately measure employee productivity, especially in regards to long-term labor contracts, such as tenure. Therefore, many universities and administrators are left trying to answer the same age old questions: Is faculty member "A" as productive as in years past? How does faculty member "A" compare to faculty member "B"? Could I replace faculty member "A's" production value with faculty member "C" at a lower cost to the university? These questions and others like them open the door to age-old concerns of disincentives associated with tenure and continue to present many university administrators with legitimate challenges in their attempts to assess faculty performance and determine how it translates into value for their institutions.

Previous research (Alchain & Demsetz, 1962; Holmstrom, 1979) has highlighted some of the issues and problems associated with multi-year labor contracts. Indeed, the literature has drawn attention to the fact that productivity often suffers as a result of long-term job security. In particular, allegations of production declines due to long-term job security have been associated with seniority rights, professional athletes, and in the academic institution of tenure (Krautmann, 1990).

Understanding and predicting the aforementioned productivity declines as it relates to tenure could prove invaluable for administrators and university leaders in motivating faculty and making policy decisions.

THEORETICAL FRAMEWORK

Perhaps the single largest determinant of productivity among workers in all facets of life is motivation. It is unlikely that higher education faculty members are an exception. It has long been thought that by taking away the proverbial carrot, one is also taking away incentive and motivation for sustained effort. Vroom's Expectancy Theory (1964) attempts to predict effort and, consequently, productivity as it relates to individual motivation.

According to Expectancy Theory of motivation (Vroom, 1964), individuals make decisions to perform based on cognitive concepts of subjective probabilities. Further, these cognitions are representative of an individual's perception of the likelihood that effort will lead to performance and performance will lead to desired outcomes. Specifically, Vroom's theory assumes that "the choices made by a person among alternative courses of action are lawfully related to psychological events occurring contemporaneously with the behavior" (1964).

The purpose of Expectancy Theory is to understand motivation in organizations and how individuals make decisions regarding various behavioral alternatives (Mitchell & Biglan, 1971; Nadler & Lawler, 1977; Porter & Lawler, 1968; Vroom, 1964). As Nadler & Lawler (1977) point out, Expectancy Theory focuses on a number of specific assumptions about the causes of behavior and performance in organizations. The assumptions are as follows: (1) behavior is determined by a combination of forces in the individual and forces in the environment, (2) people make decisions about their own behavior in organizations, and (3) different people have different types of needs, desires and goals which can influence performance.

QUANTITATIVE ANALYSIS

Pre-tenure and post-tenure data determining research productivity levels of tenured faculty members (N=24) were collected from the College of Education at a Regional University in the Southwest in order to ascertain whether Expectancy Theory predictions hold true in an academic setting. Productivity is operationally defined as research activity in the form of published journal articles. This study evaluated research productivity for three years "pre-tenure" and three years "post-tenure" for each eligible faculty member and discovered a significant ($p=0.00097$) decline in research publications for tenured faculty accounting for a 42% reduction

in scholarly publications. The results of the statistical analysis are consistent with Expectancy Theory predictions.

REFERENCES

- Alchain, A., & Demsetz, H. (1962). Production, information costs, and economic organization. *American Economic Review*, 6, 777-795.
- Holmstrom, B. (1979). Moral hazard and observability. *Bell Journal of Economics Management*, 2, 36-41.
- Krautmann, A. C. (1990). Shirking or stochastic productivity in Major League Baseball? *Southern Economic Journal*, 14, 961-968.
- Mitchell, T. R., & Biglan, A. (1971). Instrumentality theories: Current issues in psychology. *Psychological Bulletin*, 76, 432-454.
- Nadler, D. A., & Lawler, E. E. (1977). Motivation: A diagnostic approach. In J. R. Hackman, E. E. Lawler, & L. W. Porter (Eds.), *Perspectives on behavior in organizations* (pp.26-34). New York: McGraw-Hill.
- Porter, L. W., & Lawler, E. E. (1968). *Managerial attitudes and performance*. Homewood, IL: Irwin-Dorsey.
- Vroom, V. H. (1964). *Work and motivation*. New York: Wiley & Sons.

SERVANT LEADERSHIP'S IMPACT ON PROFIT, EMPLOYEE SATISFACTION, AND EMPOWERMENT WITHIN THE FRAMEWORK OF A PARTICIPATIVE CULTURE IN BUSINESS

David Jones, Southern Wesleyan University

ABSTRACT

Servant leadership has gained an enormous amount of popularity in organizations by being viewed as a promising resolution to a perceived need for leaders to become more efficient, principled, and employee focused. Yet there is paucity of empirical research to substantiate these claims. This study attempted to fill this knowledge gap. The research questions explored (a) the necessary and sufficient conditions to help maintain servant leadership in an organization; and (b) the role servant leadership might play in ensuring a participative business culture along with profitability, employee satisfaction, and empowerment. The results suggest that (a) servant leadership enhances profits through reduced turnover and increased organizational trust, and (b) employee satisfaction increases in organizations where leaders see themselves as servants first.

INTRODUCTION

Virtually all businesses, as well as other organizations, can all benefit from improved leadership and management methods. Servant leadership (Greenleaf, 1970) is one leadership approach that is increasing in popularity because of its focus on improving the organization through culture-building and empowerment; subsequently leading to greater profits for the firm. Greenleaf further indicated that the foundation of servant leadership is not established on the more traditional power model of leadership, but on the notion that by serving others and helping them to grow and to develop as individuals, institutional effectiveness can be enhanced through mechanisms such as job satisfaction, and empowerment. Greenleaf (1977) began the discussion about servant leadership by arguing that the leader should put the needs of the follower before their own needs by helping individuals to grow and improve as human beings. Graham (1999) asserted that a servant leader would focus on fulfilling the needs of the follower first, with the needs of the organization coming second, and the servant leader's needs placed last. Daft and Lengel (2000) continued the conversation by emphasizing that the aspiration of leaders to serve their followers took priority above their own ambitions to be in an official position of leadership, thereby, a viewpoint that is congruent with the fundamental tenants of servant leadership as described by Greenleaf.

Stone, Russell, and Patterson (2004) described how a follower within an organization that practices servant leadership would achieve greater personal success and subsequently develop

more deeply. Whereas, Hamilton and Bean (2005) postulated that servant leadership would effortlessly increase the progress of each follower in helping the individual to achieve their greatest level of growth and development. Consequently, the ability of an organization to compete in a very difficult business climate requires that a company have effective leadership. Greenleaf's (1977) servant leadership model places the needs of the employee first and is viewed by many (Glashagel, 2009; Sipe & Frick, 2009) as being an appropriate leadership model that leads to increased organizational performance and enhanced employee satisfaction.

Although substantial research has been conducted regarding the characteristics that define a servant leader (Spears, 1998), available research has not clearly indicated what the motivation is for an organization to sustain and maintain servant leadership. Therefore, the current research addresses specifically the perceived problem that leaders need to become more efficient, principled, and employee focused and how servant leadership has been proven to be effective once implemented and maintained in organizations (Lynham & Chermack, 2006).

LITERATURE REVIEW

Bass (2000) asserted that servant leadership would become quite significant in organizations due to its focus on the follower and the efforts of the leader to promote the independence, knowledge, and development of the individual. Mukli, Jaramillo, and Locander (2005) researched the effects that a sales leader may have on subordinates and concluded that the leader did have an influence on employee performance, thereby having a potential impact upon organizational financial results. A principal difference between the structure of leadership described by Burns (1978) and Greenleaf's (1977) servant leadership is the fact that servant leadership focuses on the needs of the follower first, as opposed to the needs of the organization or of the individual manager. Matteson and Irving (2006) supported many of the ideas forwarded by Greenleaf and Burns, although, specifically addressing servant leadership and advancing that servant leadership is fundamentally concentrated on identifying and addressing the requirements of followers ahead of individual considerations, ultimately, leading to the development and growth of the follower (Polleys, 2002).

The current research examined servant leadership and the resulting relationship between the leader and follower and what the resulting outcomes were in reference to issues such as employee satisfaction, organizational performance, organizational culture, and empowerment. Franke and Park (2006) found that servant leadership was responsible for increased satisfaction levels of employees and greater commitment to the organization. Mayer, Bardes, and Piccolo (2008) showed increased employee performance when an employee viewed their manager as a servant leader, with attributes including: trust, empowerment, acceptance, empathy, positive morale, and the desire to serve others were a number of the traits that would formulate a good leader and follower relationship, according to Greenleaf (1970). From this idea of servant leadership, Greenleaf promoted the goals, aspirations, and interests of the followers to the forefront of the organization. At its core, the servant leadership model shares similarities with more established leadership models such as transformational leadership. However, the primary unique feature of servant leadership compared to all others is the emphasis that is placed on

helping the follower to grow and develop. Greenleaf (2002) hypothesized that servant leadership positions the leader in an arrangement within a group, whereby, the leader is not the central focus of the group, allowing resources and support to be provided to followers. Therefore, servant leaders would be motivated primarily by an intrinsic desire to serve, rather than being motivated simply by power.

Accordingly, Greenleaf (1970) described that a primary motivation of servant leaders evolves from an underlying attitude of social responsibility and equality. Liden, Wayne, Zhao, and Henderson (2008) expressed that a servant leader may be viewed from a perspective of being moral and that the servant leader sincerely believes that he or she is not superior to any other member of the organization. Servant leaders demonstrate authenticity in leadership by operating as trustees of the organization who facilitate the development and growth of community between members of an organization (Greenleaf, 1977). Additionally, altruistic calling, emotional healing, wisdom, persuasive mapping, and organizational stewardship were all categorized as servant leadership traits (Barbuto & Wheeler, 2006). Guenzi, Catherine, and Laurent (2007) furthered described the need to identify and effectively clarify what characteristics a servant leader possessed. Ultimately, outcomes that would positively impact the organization, such as extra effort by the employee, greater employee satisfaction, and improvements in the overall effectiveness of the company were determined to be realistic goals that when introduced, benefited the company through better financial performance through servant leadership.

METHODOLOGY

Interview-driven, qualitative research and analysis was determined to be suitable for this study because it enabled the pursuit of two goals: (a) understanding the impact of servant leadership on the employees of a business or organization, and (b) comprehending the necessary and sufficient characteristics for sustaining servant leadership within the organization. In-depth interviews were conducted for the purpose of investigating the effects of servant leadership and its impact within organizations, the influence on employees, and its bottom line implications.

Criteria related to sales revenues, employee satisfaction, turnover, insurance claims, budget requirements, and even community reputation were all areas that the participant generally needed to have strong data on in order to provide a sufficient amount of necessary information in the interviews so that a detailed analysis and interpretation could be conducted and subsequently concluded. Participants that matched the specified criteria were chosen and consisted of 21 proprietors, leaders, and employees of various businesses and organizations. In keeping true to the specified criteria, the participants consisted of: ten CEO's, three presidents, six senior vice-presidents, one professor, and one author. It should be noted that both the author and the professor have experience implementing servant leadership. The organizations researched and the individuals that participated in the study were self-identified as servant leaders, or as being in organizations that have followed the servant leadership model from 3 years to more than 40 years, thus giving all of the participants experience with the model of servant leadership.

RESULTS AND CONCLUSIONS

The data certainly suggested that servant leadership within an organization has very positive benefits and affirmative outcomes. These outcomes led to certain themes that included a reduction in turnover among organizations employees, profitability increases, and how trust developed and grew between the organization and the follower. Other results determined from the data indicated that both implementation and sustaining of servant leadership was required from the top management. Additionally, culture was determined to be developed from within the organization and that a concern for others was viewed as an absolute necessity for sustaining and maintaining servant leadership. Finally, empowering others was seen as a positive means to strengthen the organization.

REFERENCES

- Barbuto, J., & Wheeler, D. (2006). Scale development and construct clarification of servant leadership. *Group & Organization Management* 31(3), 300-327.
- Bass, B. M. (2000). The future of leadership in learning organizations. *Journal of Leadership Studies*, 7, 18-40.
- Burns, J. M. (1978). *Leadership*. New York, NY: Harper & Row.
- Daft, R. L., & Lengel, R. H. (2000). *Fusion leadership: Unlocking the subtle forces that change people and organizations*. San Francisco, CA: Berrett-Koehler.
- Franke, George R., & Jeong-Eun Park (2006). Salesperson Adaptive Selling Behavior and Customer Orientation: A Meta-Analysis. *Journal of Marketing Research*, 43 (November), 693–702.
- Glashagel, J. (2009). *Servant institutions in business*. Westfield, IN: Greenleaf Center for Servant Leadership.
- Graham, J. (1999). Servant leadership in organizations: Inspirational and moral. *Leadership Quarterly*, 2, 105-119.
- Greenleaf, R. K. (1970). *The servant as leader*. Westfield, IN: The Robert K. Greenleaf Center.
- Greenleaf, R. K. (1977). *Servant leadership: A journey into the nature of legitimate power and greatness*. New York: Paulist Press.
- Greenleaf, R. K. (2002). *Servant leadership*. Mahwah, NJ: Paulist Press.
- Guenzi, P., Catherine, P., & Laurent, G. (2007, January). Relational Selling Strategy and Key Account Managers' Relational Behaviors: An Exploratory Study, *Industrial Marketing Management*, 36, 121–133.
- Hamilton, F., & Bean, C. (2005). The importance of context, beliefs and values in leadership development. *Business Ethics: A European Review*, 14(4), 336-347.
- Liden, R. C., Wayne, S. J., Zhao, H., & Henderson, D. (2008). Servant leadership: Development of a multidimensional measure and multi-level assessment. *Leadership Quarterly*, 19, 161–177.
- Lynham, S. & Chermack, T. (2006). Responsible leadership for performance: A theoretical model and hypotheses. *Journal of Leadership & Organizational studies*, 12(4), 73-88.
- Mayer, D., Bardes, M., & Piccolo, R. (2008). Do servant-leaders help satisfy follower needs?
- Mulki, J., Jaramillo, F., & Locander, W. (2005). Transform or transact? Which leader gets better results? A meta-analysis. *Journal of Business and Leadership: Research, Practice, and Teaching*, 1(1), 85-94.
- Polleys, M. S. (2002). One university's response to the anti-leadership vaccine: Developing servant leaders. *Journal of Leadership Studies*, 8(3), 117-130.
- Sipe, J., & Frick, D. (2009). *Seven pillars of servant leadership*. New York: Paulist Press.
- Spears, L. C. (Ed.). (1998). *Insights on leadership: Service, stewardship, spirit, and servant leadership*. New York, NY: John Wiley & Sons.
- Stone, A. G., Russell, R. F., & Patterson, K. (2004). Transformational versus servant leadership: A difference in leader focus. *Leadership & Organizational Development Journal*, 25(3/4), 349-361.

GOING WHERE ANGELS FEAR TO TREAD: AUCTIONING UNIVERSITY PARKING TO ENHANCE REVENUE

Michael A. McCollough, University of Idaho

Steven R. Shook, University of Idaho

ABSTRACT

On most university campuses Parking and Transportation Services (PTS) is a self-sustaining auxiliary unit. In an era of declining state support for higher education, auxiliary units are increasingly charged with maximizing revenue and profits. This study reports on research undertaken at a medium-sized, state-assisted university to determine price sensitivity by parking permit type and market receptivity to the auctioning of parking spaces. While rare, some universities have examined the possibilities of auctioning university (Gadsby et. al 2003) parking and this research builds on their experiences.

Based on a sample of 1,220 (25% response rate) faculty, staff, administrators, and students, it was determined via conjoint study that the current permit system significantly underprices all the preferred parking permits. Faculty would be willing to pay approximately twice what they currently pay for a 24/7 reserved space in the most desirable lots (\$630 versus \$312). Interestingly, students and staff would pay as much as \$1,400 for a reserved space in a premium lot versus the current \$156 for a parking permit in student-staff lots). Overall, among students there was a negative correlation between what they would pay in an auction for a reserved space and their income level, likely reflecting the impact of financial aid and their income constraints. Further, as students incur the most parking fines, some students no doubt view it as rational to pay significantly more for a permit that eliminates their parking fines.

Obstacles to an auction system however are significant. Operationally, online auction websites such as eBay do not allow private auctions. Therefore, auction software must be internally developed or purchased through a vendor. Most significantly are the nonmonetary costs to the institution of implementing an auction. Many in the university community view parking as a right because it is felt as being a requirement for enrollment or employment. Therefore, some view an auction system as repugnant, despite the fact that the low demand, least desirable lots would remain available at a nominal charge and these lots are within a twelve minute walk to the most distant building on campus. Nevertheless, many regard access, or rather the right to hunt for convenient parking as a right and are skeptical of pricing based on what the market will bear. However, against this attitude is a growing awareness that as universities evaluate their sustainability practices they are finding that parking lots are often run at a loss, can discourage car pooling or taking the bus, and impact the amount of automobile congestion on campus while reducing green space (Burr 2011). Indeed, across the nation it is estimated that there is more capital invested in parking lots than in the vehicles that occupy these parking

spaces (Shoup 1997). Further, as some universities attempt to increase enrollments to offset declining state revenues, the pressure on the parking infrastructure increases at the same time that funds are unavailable to construct and maintain new lots (Chance 2006, Millard-Ball 2004). Therefore, pricing to market provides not just a means for a university to increase revenues but also to practice its environmental sustainability mandate and deal with increased enrollments.

A further problem with auctioning reserved permits is that it would reduce the effective utilization of lots, resulting in prime lots that are now full during peak hours having significantly more open spaces. Such dead time in essence reflects suboptimal use of existing infrastructure (Epstein 2002). While the market based alternative of implementing hourly parking rates (i.e., parking meters) would likely maximize revenues, it would also be extremely unpopular with all members of the university community.

Based on the research conducted, it is recommended that the university launch a pilot, English-style auction in select lots to gauge actual demand. Investment in the auction software that must be developed can be recovered it is estimated in the first year with a significant positive return-on-investment. Further, the possibility exists to license the software to other institutions.

REFERENCES

- Burr, D. (2011). Is university parking a common grievance? *Parking Today*, 16(9), 32-33.
- Chance, B. (2006). Higher ed parking funded by outdated procedures. *Parking Today*, 11(9), 35.
- Epstein, R.A. (2002). The allocation of the commons: parking on public roads. *The Journal of Legal Studies*, 31(S2), 515-544.
- Gadsby, E., Jaimes, S., Najarian, L., Sanchez, M., Sujlana, R., Donohue, G.L., Coyne, M., (2003). George Mason University (GMU) Fairfax campus transportation system. *Systems and Information Engineering Design Symposium*, 77-82.
- Millard-Ball, A. (2006). Solving parking shortages: New solutions for an old problem. *Planning for Higher Education*, 33(1), 30-43.
- Shoup, D.C. (1997). The high cost of free parking. *Journal of Planning Education and Research*. 17, 3

THE BIGGEST THREAT TO THE U.S. DIGITAL INFRASTRUCTURE: THE CYBER SECURITY WORKFORCE SUPPLY CHAIN

Aleta Wilson, University of Maryland University College
Amjad Ali, University of Maryland University College

ABSTRACT

This research examines the issue of supply and demand for cybersecurity professionals to determine how to optimize the output of cybersecurity professionals through a supply chain. It was found that progress is impeded by the lack of a clearly defined and standardized definition of a cybersecurity worker and their associated knowledge, skills, and abilities. There is a known shortage of cybersecurity professionals that is affecting the ability of the United States to fulfil the mandate of President Obama who declared that the protection of our digital infrastructure is a national security priority. The problem with this declaration is that a literature review confirms there is no standard definition of a cybersecurity worker, associated skills, or educational requirements. The cybersecurity workforce to which we speak in this report consists of those who self-identify as cyber or security specialists as well as those who build and maintain the nation's critical infrastructure. Considering the criticality of the national infrastructure, it is time for the US to take immediate steps to coordinate the development of the cybersecurity field and its associated workforce supply chain.

INTRODUCTION

There is a shortage of cybersecurity professionals that is affecting the ability of the United States to fulfil the mandate of President Obama who declared that the protection of our digital infrastructure is a national security priority (Obama, 2009). Trade associations, and Congressional committees have been holding discussions on this issue for several years, but the traditional supply chain method for meeting employer needs is unresponsive in the short term.

SCOPE

The scope of this research encompasses two areas. The first is cybersecurity professionals in the federal government and its contractor community, because government agencies such as the National Institute of Standards and Technologies (NIST) and the Department of Homeland Security (DHS) promulgate regulations associated with technology workers and these regulations frequently form the model or basis for private sector organizations. The second focus of this research is university level education and certifications as part of the supply chain that provides cybersecurity professionals. Supply chain management is used in this research to view how

these workers get to the workplace, and to explore how to optimize the supply chain to increase production.

DEFINITION OF A CYBERSECURITY WORKER

Before one can understand the problem, it is first necessary to define a cybersecurity professional. The term is freely used while no one has a clear definition. The rapid evolution of technology is racing ahead of our federal human resource classification systems. Even the Occupational Outlook Handbook put out by the U.S. Bureau of Labor Statistics (BLS), does not contain a definition for cybersecurity professionals (U.S. Department of Labor [DOL], 2010-2011). The Handbook lists Information technology workers under the category of "Computer and mathematical occupations" with nine subcategories.

Some Handbook subcategories acknowledge positions that involve people who "plan, coordinate, and maintain an organization's information security" and "database administrators also must plan and coordinate security measures with network administrators", and network engineers "may ... address information security issues" (DOL 2010-2011)."

Department of Homeland Security (DHS) Secretary Janet Napolitano defines Cybersecurity professionals as employees responsible for "... cyber risk and strategic analysis; cyber incident response; vulnerability detection and assessment; intelligence and investigation; and network and systems engineering" (Krebs, 2009). Frost & Sullivan conducted a survey of 10,413 information security professionals (Ayoub, 2011), which indirectly defined security professionals as those "employed as Information Security professionals and those who had cyber security as their primary job function.

The cybersecurity professional addressed in this report consists of professionals who have information security as a major part of their job; those who self-identify as cyber or security specialists; and, those who build and maintain the national critical infrastructure of the computer systems on which the public and private sectors have come to rely.

NEED FOR CYBERSECURITY PROFESSIONALS

The DHS gave Secretary Janet Napolitano hiring authority to staff up to 1,000 positions over three years, and the recently established Cyber Command with responsibility for overseeing government efforts to protect the military's computer networks, will be competing with DHS for cyber staff (U.S. Department of Defense, 2011; Krebs, 2009).

In 2008, the President acknowledged in a Presidential Directive that "... there are not enough cybersecurity experts within the Federal Government or private sector to implement the [Comprehensive National Cybersecurity Initiative], nor is there an adequately established Federal cybersecurity career field" (Obama, 2009).

The "federal government's cybersecurity workforce is broken, facing a serious shortage of trained personnel, an over-reliance on contractors and a hiring process that doesn't attract the right candidates", according to a new report from the non-profit Partnership for Public Service (Partnership for Public Service & Booz Allen, 2009). In addition to the apparent shortage, many

CIOs and CISOs complain about the lack of skilled candidates that apply for federal cybersecurity jobs. "Thirty-three percent said they were upset with the quality of applicants and more than a third said they weren't able to collaborate enough with HR managers" (Carlstrom, 2009).

The Partnership also found problems with the scholarship programs designed to attract students to federal cybersecurity jobs. One program, Scholarship for Service (SFS), graduates about 120 students each year — but it needs to generate 500 to 1,000 graduates per year to meet the government's needs (Carlstrom, 2009). The SFS program pays full tuition plus a stipend and students must work for a federal agency for a time period equal to the length of the scholarship.

WHAT CYBER SKILLS ARE NEEDED

A Frost & Sullivan survey found that "Cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security" (Ayoub, 2011). Interestingly, more than 50% of the survey respondents say they have private clouds in place, while 70% of those who have implemented cloud computing lack the staff with required skills to properly secure cloud-based technologies. Specific needs identified in the Frost and Sullivan survey are 1) a detailed understanding of cloud computing; 2) enhanced technical knowledge; and, 3) contract negotiation skills. It is interesting to note that contract negotiation skills have been added due to the movement of infrastructure hardware and software to the cloud, which necessitates an understanding of contracts to address such issues as placement and movement of data across networks and geographies.

Essentially, this means that the current IT workforce is not keeping up with the rapidly evolving technological frontiers. Goslers, Fellow at Sandia Labs, postulates a more generic set of skill requirements that includes: 1) fundamentals of technology; 2) well versed in how technology is implemented; and 3) have a strong understanding of how vulnerabilities can be introduced (Gjelten, 2010).

SUPPLY CHAIN MANAGEMENT

Applying the concept of supply chain management (SCM) to a study of the Cybersecurity workforce is not a novel approach. In fact, Capelli (2009) argues that SCM for human resources is an excellent approach that attacks the problem of uncertainty head-on. IBM, manages its staffing problems by automating an SCM process specifically designed to predict its staffing needs. Its system, Resource Capacity Planning (RCP) Optimizer, is designed to solve two core resource planning problems---shortages (gaps) and excesses (gluts) (Gresh, Connors, & Fasano, 2007).

The problem for the federal government is that, unlike IBM, a single entity, the federal government is composed of numerous agencies, sub-agencies, and directorates each with their own internal systems. Therefore, it would be difficult to develop an automated methodology to satisfy all of the federal governments needs. But, it is possible for a single agency to predict its needs and those individual agency predictions could be rolled up into a good overall estimate.

Human Resources (HR) supply chains are typically composed of all activities involved in fulfilling staffing requests. At the highest level, the customer for cybersecurity professionals is the federal government and its contractor community. In the case, of the cybersecurity workforce supply, the supply chain can extend from pre-kindergarten through university, certifications, training, and other life-long learning opportunities.

K-12 Education (STEM)

The issues related to the beginning of the supply chain, K-12, are being addressed through the Obama administration's push for increased emphasis on education in science, technology, engineering, and math (STEM). The STEM campaign involves a public-private partnership with over \$260M invested over the next decade (Obama, 2009). This mandate is being compared to the investment the United States made in engineering for the race to the moon, during the Kennedy administration. In fact, growth in STEM jobs was three times as fast as growth in non-STEM jobs during the last 10 years. Unfortunately, the results of STEM investment may not begin to surface for ten years.

University Level Education

The cybersecurity workforce problem is being addressed at the university level through Center's of Academic Excellence outreach efforts designed and operated by the National Security Agency (NSA) in the spirit of Presidential Decision Directive 63 (PDD 63), and the Clinton Administration's Policy on Critical Infrastructure Protection (CIP) (Clinton, 1998; NSA, 2010b). The CIP program goal is to reduce vulnerability in our National Information Infrastructure by promoting higher education in information assurance (IA), and to produce a growing number of professionals with IA expertise in various disciplines.

As of 2010, there were one hundred twenty-four (124) National Center's of Excellence certified by the National Security Agency, Central Security Service (NSA, 2010a). Fourteen (14) of the Centers are 2-year institutions providing Information Assurance (IA) education. Two (2) are 4-year institutions providing IA education, and fifty-one (51) are institutions that integrate research activities into the curriculum (NSA, 2009). It should be noted that some institutions fall into more than one category, therefore, they do not add up to the total of one hundred twenty-four. These institutions offer both degree and certificate programs and the length of each program varies depending on the offering institution.

The overarching problem is time. Neither the STEM initiatives, National Center's of Academic Excellence, or scholarships can produce the cybersecurity talent that is needed now. "The current rate of production of skilled cyber-security workers satisfies the appetite of neither the public nor private sector, and if we do not make a concerted effort to drastically increase this work force, then the U.S. will export high-paying information security jobs" (Locasto, Ghosh, Jajodia, & Stavrou, 2011).

Certifications

At some point, professionals in a computer related industry decide whether they want to obtain some type of cybersecurity certificate as a way to advance their career, and this decision may be prompted by employer requirements. There are a variety of organizations that offer certifications, and they essentially come from one of two sources---Higher educational institutions and non-higher educational institutions with the later being composed of dot-orgs and for-profits. The most widely known and popular are the Certified Information Systems Security Professional (CISSP) governed by the International Information Systems Security Certification Consortium (ISC)², and the Global Information Assurance Certifications (GIAC). The CISSP has become the defacto industry standard that was adopted as a baseline for the U.S. National Security Agency's Information Systems Security Engineering Professional (ISSEP) program, while the GIAC certifications come from the SANS Institute which is a research and educational institution for security professionals.

CONCLUSION

The field of cybersecurity and the cyber workforce is being developed in pieces. The National Institute of Standards, Carnegie Mellon, International Information Systems Security Certification Consortium (ISC)², Microsoft, Cisco, and NSA are each designing and developing standards, models, processes, certifications, and methodologies for portions of the cybersecurity field, and many of them overlap, and all of this is effecting the cybersecurity profession.

The development of a supply chain for cybersecurity professionals begins with development of a clearly defined career field based upon a definition that can be developed by and agreed upon by both government and industry. Once the career field roadmap is completed, then other portions can begin to develop in a coordinated fashion: degrees and their courses can be planned; estimates on workforce needs can more accurately be determined; and, training and certifications can be organized and synchronized.

Considering the criticality of the national infrastructure, it is time for the US to take immediate steps to coordinate the development of the cybersecurity field and its associated workforce supply chain.

REFERENCES

- Assante, M. J., & Tobey, D. H. (2011, January/February). Enhancing the Cybersecurity Workforce. *IT Professional Magazine*, 13, 12-15.
- Ayoub, R. (2011). The 2011 (ISC)² Global Information Security Workforce Study. In ISC2 (Ed.), (pp. 1-26): Frost & Sullivan.
- Carlstrom, G. (2009, July 22). Too few in pipeline for cybersecurity jobs, CIOs complain. *Federal Times*. Retrieved from <http://www.federaltimes.com/article/20090722/IT01/907220302/-1/RSS>
- Clinton, B. (1998). Presidential Decision Directive/NSC-63, from <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>
- Gjeltén, T. (Producer). (2010). Cyberwarrior shortage threatens U.S. Security [Radio]. In T. Gjeltén (Producer): National Public Radio.

- Gresh, D. L., Connors, D. P., & Fasano, J. P. (2007). Applying supply chain optimization techniques to workforce planning problems. *IBM Journal of Research and Development*, 51(3/4), 251-261.
- Krebs, B. (2009). DHS Seeking 1,000 Cyber Security Experts. *Washington Post* [Blog]. Washington, DC.
- Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). Virtual Extension The Ephemeral Legion: Producing an Expert Cyber-Security Work Force from Thin Air. [Opinion]. *Communications of the ACM*, 54(1), 129-131.
- NSA. (2009). Information Assurance, Centers of Academic Excellence Retrieved July 22, 2011
- NSA. (2010a). Centers of Academic Excellence Retrieved May 28, 2011, 2011, from http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml
- NSA. (2010b, September 10, 2010). National Centers of Academic Excellence Retrieved May 28, 2011, 2011, from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml
- Obama, B. (2009). Securing Our Nation's Cyber Infrastructure, Speech by President Obama, May 29, 2009, 2011, Retrieved from http://www.whitehouse.gov/the_press_office/remarks-by-the-president-on-securing-our-nations-cyber-infrastructure
- Partnership for Public Service & Booz Allen. (2009). Cyber In-security: Strengthening the Federal Cybersecurity Workforce. Washington: Partnership for Public Service and Booz, Allen, & Hamilton. Retrieved from www.ourpublicservice.org/OPS/publications/download.php?id=135
- U.S. Department of Labor. (2010-2011). *Occupational Outlook Handbook, 2010-2011 Edition, Bulletin 2800* (2010-2011, Bulletin 2800 ed.). Washington, DC: U.S. Government Printing Office, Washington, DC, 2006.
- U.S. General Accountability office. (2011b). Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates (pp. 33). Washington, DC: General Accountability Office.
- U.S. Department of Defense. (2011). DOD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander Retrieved May 27, 2011, 2011, from <http://www.defense.gov/releases/release.aspx?releaseid=13551>
- U.S. Office of Personnel Management. (2002). General questions and answers about OPM background investigations Retrieved June 4, 2011, 2011, from http://www.opm.gov/products_and_services/investigations/faqs.asp
- Wilson, M., Stine, K., & Bowen, P. (2009). Information Security training Requirements: A Role- and Performance-Based Model (Draft): (pp. 157). Gaithersburg: National Institute of Standards and Technology.