Bridging the Security Gap between Software Developers and Penetration Testers: A Job Characteristic Theory Perspective

Emergent Research Forum (ERF)

Hwee-Joo Kam
University of Tampa
hkam@ut.edu

Vishal Shah
Central Michigan University
shah3v@cmich.edu

Shuyuan Mary Ho
Florida State University
smho@fsu.edu

Abstract

Building on Job Characteristics Theory (JCT), this article suggests that job characteristics differ between software developers and penetration testers; and subsequently, this generates different levels of job motivation related to information security protection between these groups. This study proposes a research model based on JCT to examine the differences in job motivation between software developers and penetration testers. Insights gained from the research model can be used to: (1) bridge the security gap between software development and penetration testing for alleviating software vulnerabilities and (2) propose viable suggestions to promote mutual understanding between both professional groups for improving software security. Moving beyond the propositions offered by the research model, this study will design and build a laboratory experiment to capture the actual behaviors related to job motivation.

Keywords

Secure software, penetration testing, software vulnerabilities, and job motivation.

Introduction

Software vulnerabilities is a thorny issue. The 2016 Internet Security Threat Report revealed that a malicious code identified as XcodeGhost was found in the Apple's development environment, placing users of iOS applications at risk (Symantec 2016). Despite the risk posed by software vulnerabilities, Ponemon Institute (2012) reported that 44% of developers surveyed claimed to have no collaboration with information security (InfoSec) professionals in their organizations. Modern software development does not incorporate software security (Tryfonas, Kiountouzis & Poulymenakou 2001), undermining InfoSec.

Because software security is not a stand-alone problem but an organization-wide issue (Van Wyk & McGraw 2005), it is important for different professional groups in an organization to build mutual understanding about Information Security (InfoSec). Such understanding may lead to a productive dialogue and collaboration towards assuring software security. In general, secure software development encompasses a wide range from planning to deployment. To build secure software systems, all groups who are involved in the phases of the software development life cycle (SDLC) should reach a consensus on the software security issues. This is especially applicable to the two major groups involved in secure software development: (a) Software developers (2) InfoSec professionals such as penetration testers.

Given the different viewpoints about security among the aforementioned groups (Tøndel, Jaatun, and Meland 2008), a "security gap" emerges between software developers and InfoSec professionals (Van Wyk & McGraw 2005), such as penetration testers. Such a security gap could have undesirable consequences (Mouratidis, Giorgini, & Manson 2005), as it can compromise software system, exposing vulnerable data. In order to reduce the security gap, it is important to know why each group exhibits a

certain job behavior towards security issues in software development (Van Wyk & McGraw 2005). Accordingly, this study applies Job Characteristics Theory of Work Motivation to examine the differences in job motivation between software developers and penetration testers. Main objectives of our long-term research project are: (1) discover the mechanisms explaining different security behaviors between the Software and InfoSec professional groups and (2) provide managerial implications to improve the information flow between software developers and penetration testers about software security issues.

Literature Review

Several theories in the extant literature explain job performance, attitudes, behavior, and motivation. To begin with, Valance, Instrumentality, and Expectancy (VIE) model suggests that an employee is motivated to perform a job when he or she expects that his or her action will produce a positive outcome (Vroom 1964). Additionally, Goal Setting Theory (Locke & Latham 1990) posits that there is a positive relationship between goal difficulty and task performance as long as the person involved has committed to the goal, has no conflicting goal, and can achieve the goal.

Moreover, Salancik & Pfeffer (1978) proposed Social Information Processing (SIP) theory to explain human behavior and attitude at work. SIP suggests that employee satisfaction is formed by discriminately perceiving and interpreting their social environment and past actions (Salancik & Pfeffer 1978). In the same vein, Social Exchange Theory (SET) (Blau 1964) focuses on the social context in term of exchange relationships among actors. SET suggests that norms of reciprocity governs social exchange and shapes work attitudes and behaviors (Settoon, Bennett, & Liden 1996). On the other hand, Self-Determination Theory (SDT) proposes that individuals are intrinsically motivated to perform the activities if they develop a high degree of internalization related to the activities (Gagne & Deci, 2005). When individuals internalize the activities, they will develop an emotional tie with the activities, and subsequently, they are intrinsically motivated to engage in the job activities.

Software development, as well as its testing, tend to be solitary work for a large part. Besides, we plan to test our research on individual software developers and researchers. These individuals are likely not restricted to a corporation. Hence, there is no effective way to measure social exchange for the two groups. Thus, theories that deal with job motivation are of interest to our work. More specifically, it would be worthwhile to discover factors that lead to job motivation and compare them across two groups. To do so, we draw on Job Characteristics Theory (JCT) of Work Motivation (Hackman & Oldham 1976).

JCT posits that job characteristics shape worker's mental states that later produces job motivation (Hackman & Oldham 1976). Therefore, we argue that JCT applies to this study that examines how the differences in job characteristics engender the differences in job motivation. JCT is adopted in the organizational behavior literature to study the relationship between job characteristics and job burnout (Maslach & Jackson 1981; Demerouti et al. 2001). In the Information Systems (IS) research, a study proposed using JCT to examine the differences in job dimensions between IS contractors and permanent IS professionals in a software development team (Ang & Slaughter 2001). Moreover, Baddoo & Hall (2002) adopted JCT to investigate the motivating factors that drove developers, project managers, and senior managers to engage in software process improvement. Building on JCT, Thatcher et al. (2006) investigated how intrinsic motivation affects IT worker's attitudes and intentions. Finally, Venkatesh & Davis (2000) used JCT to justify a relationship between result demonstrability (i.e. the degree of result's tangibility for a system) and perceived usefulness (i.e. the degree of perception related to the usefulness of a system) in a study that examined user's acceptance of the technology.

Theoretical Framework

Referring to JCT (Hackman & Oldham 1976), employees performing their tasks under the same job description are more likely to share similar job dimensions, thus leading to similar perceptions toward their jobs and responsibilities. Consequently, this may lead to similar job motivation and behaviors. In contrast, a different job description may produce different job dimensions, thus resulting in different job-related perceptions that may usher in a different set of job motivations and behaviors. For example, software developers develop software to enable certain functionalities; and therefore, developers may have perceived that their top priority is to write software components that support the designated functionalities. This will then motivate them to create and improve the software function (Hertel, Niedner & Herrmann 2003) rather than focusing on software security (Tøndel, Jaatun, and Meland 2008). In

contrast, a penetration tester's main duty is to discover software vulnerabilities in an organization's IT systems, and subsequently, recommend mitigation steps to improve software security in the organizational settings. Accordingly, penetration testers are motivated to search for security holes rather than focusing on the software functionality. Hence, we propose:

P1: There is a significant difference in job motivation related to information security protection between software developers and penetration testers.

In particular, JCT posits that job characteristics/dimensions shape worker's mental states (i.e. critical psychological states) that later produces the work outcomes encompassing job motivation (Hackman & Oldham 1976). One of the critical psychological states entails experienced meaningfulness of work, referring to the extent of a work's value and worthiness perceived by individuals (Hackman & Oldham 1976). For example, experienced meaningfulness of work can refer to the extent of values and worthiness of penetration testing perceived by penetration testers or the extent of values of software development perceived by software developers. Additionally, the job dimensions that are relevant to JCT are *skill variety, task identity, task significance, worker's autonomy, and feedback*.

Skill variety refers to the extent of the diverse skill sets and talents required to complete a set of different activities (Hackman & Oldham 1976). Hackman & Oldham (1976) proposed that skill variety shapes experienced meaningfulness of work. In other words, if penetration testers possess a variety of skills (i.e. scripting and hacking skills) to complete their tasks (i.e. hacking database), they would perceive that their jobs are valuable and worthwhile. Similarly, if software developers require more than coding skills (such as database design skills) to complete their tasks, they would also perceive their jobs as meaningful.

P2: Skill variety positively impacts experienced meaningfulness of the work

Task identity refers to the extent to which workers identify with the job from the beginning until the end of the work cycle (Hackman & Oldham 1976). It pertains to how much penetration testers or software developers get involved in the work processes (i.e. penetration testing or software development) since the inception until the end of a project. Task identity builds experienced meaningfulness of work (Hackman & Oldham 1976). For example, if developers perceive that they have actively participated in most of the phases in SDLC, they would perceive that their works are meaningful. Similarly, if penetration testers perceive that they have actively participated in most of the phases in penetration testing (i.e. from reconnaissance to report writing), they would also feel that their works are worthwhile.

P3: Task identity positively impacts experienced meaningfulness of the work

Task significance refers to the positive impact that a job can have in the lives of the other individuals (Hackman & Oldham 1976). Task significance leads to the experienced meaningfulness of work (Hackman & Oldham 1976). For example, if software developers or penetration testers perceive that their software security skills will help to protect national critical infrastructure, they would perceive that their works are meaningful and worthwhile.

P4: Task significance positively impacts experienced meaningfulness of the work

Worker's Autonomy refers to how much freedom a worker has in deciding his or her schedules and tasks (Hackman & Oldham 1976). For instance, this can refer to how much freedom a penetration tester has in planning his or her tests (i.e. hacking attempts) on a company's database. Worker's Autonomy builds experienced responsibility for the outcome of work, which pertains to how far individuals feel that they are personally accountable for the results of their works (Hackman & Oldham 1976). If penetration testers or software developers perceive that they have the freedom to decide their tasks, they would be more likely to hold themselves accountable for the results of their works.

P5: Worker's autonomy positively impacts experienced responsibility for outcome of the work

The last job dimension is feedback. It refers to the degree of clear and direct information about a worker's effectiveness in his or her job (Hackman & Oldham 1976). Feedback can be delivered by the direct outcomes of penetration testing or software development. For example, when software developers try to test a software function, they can tell immediately if their codes/program support the function. Also, penetration testers could immediately realize if their attempts of SQL Injection (one of the database hacking techniques) succeed by referring to the feedback provided by the database system. In this respect,

when the workers receive direct and clear feedback about the effectiveness of their works, they would obtain the knowledge of the actual results for their works (Hackman & Oldham 1976).

P6: Feedback positively impacts knowledge of actual results of the work activities

Experienced meaningfulness of work drives job motivation (Hackman & Oldham 1976). When software developers or penetration testers feel that their jobs are meaningful, they will be motivated to work.

P7: Experienced meaningfulness of the work positively impacts job motivation

Additionally, experienced responsibility for outcome drives job motivation (Hackman & Oldham 1976). When software developers or penetration testers perceive that they are held accountable for their results of their jobs, they will be motivated to do their jobs.

P8: Experienced responsibility for outcome of the work positively impacts job motivation

Hackman & Oldham (1976) also posited that knowledge of actual results of the work drives job motivation. For instance, when software developers realize their syntax or logical errors in their codes, they will be motivated to fix the errors. Similarly, when penetration testing realize what they have done something wrong in launching an attack, they will be motivated to correct their mistakes.

P9: Knowledge of actual results of the work activities positively impacts job motivation

Finally, we propose that job motivation drives actual job behavior. Prior research suggested that motivation generates positive impacts on attitude, cognition, and behavior (Vallerand, 1997). Accordingly, we contend that motivation related to information security protection creates a positive impact on security behavior, thereby encouraging individuals to protect information security in their jobs.

P10: Perceived job motivation of information security protection drives actual behavior of information security protection[1]

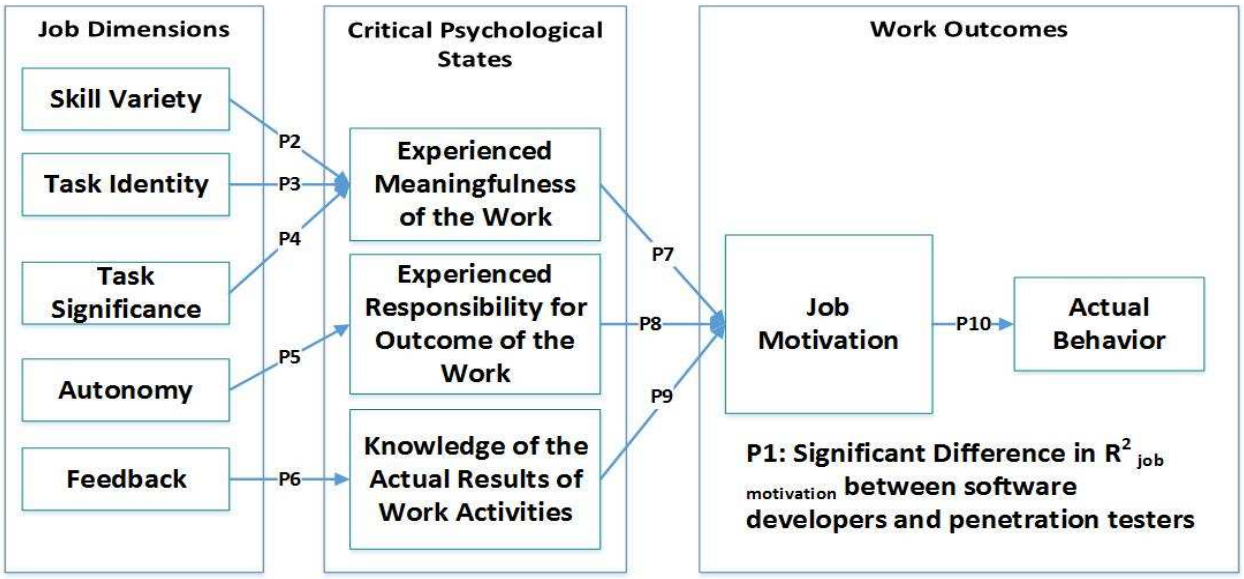

Figure 1: Adapted Model of Job Characteristics Theory of Work Motivation

Conclusion and Future Research

This study adopts the Job Characteristics Theory (Hackman & Oldham 1976) to study the differences in job behaviors between software developers and penetration testers to bridge the security gap between

[1] Proposals P2 to P10 apply to both groups. At this point, we are not proposing group difference hypothesis. Our primary function is to investigate differences in job motivation of the two groups. In our subsequent work, we will travelers back the causal chain and explore group differences among other constructs.

software development and penetration testing. There are two possible contributions of this study. First, this study will extend behavioral science research rooted in JCT to the field of information security, thereby providing a novel theoretical foundation to the Information Systems Security (ISS) studies. Second, this is one of few studies in the ISS research examining the perceptions among the professional groups. As the target group of this research are the professional groups who work in developing software products, the results can translate into actionable insights. Hence, the managerial implication of this study will go beyond generalized recommendations and will benefit the information security communities as a whole. Our next step is to design a laboratory experiment to capture the actual behavior of both groups (i.e., software developers and penetration testers) and then launch a pilot study using online questionnaires to test the proposed research model (see figure 1).

REFERENCES

Ang, S., & Slaughter, S. A. (2001). Work Outcomes and Job Design for Contract versus Permanent Information Systems Professionals on Software Development Teams. *MIS Quarterly*, 25(3), 321–350.

Blau, P. M. (1964). Exchange and Power in Social Life. London, UK: Transaction Publishers.

Baddoo, N., & Hall, T. (2002). Motivators of Software Process Improvement: An Analysis of Practitioners' Views. *The Journal of Systems & Software*, 62(2), 85–96.

Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The Job Demands-Resources Model of Burnout. *Journal of Applied Psychology*, 86(3), 499.

Gagne, M., & Deci, E. L. (2005). Self-determination theory and work motivation. Journal of Organizational Behavior, 26(4), 331–362.

Hackman, J. R., & Oldham, G. R. (1976). Motivation through the Design of Work: Test of a Theory. *Organizational Behavior and Human Performance*, 16(2), 250–279.

Hertel, G., Niedner, S., & Herrmann, S. (2003). Motivation of Software Developers in Open Source Projects: An Internet-Based Survey of Contributors to the Linux Kernel. *Research Policy*, 32(7).

Locke, E. A., & Latham, G. P. (1990). *A Theory of Goal Setting & Task Performance* (Vol. xviii). Englewood Cliffs, NJ, US: Prentice-Hall, Inc.

Maslach, C., & Jackson, S. E. (1981). The Measurement of Experienced Burnout. *Journal of Organizational Behavior*, 2(2), 99–113.

Mouratidis, H., Giorgini, P., & Manson, G. (2005). When Security Meets Software Engineering: A case of Modelling Secure Information Systems. *Information Systems*, 30(8), 609–629.

Ponemon Institute. (2012). *2012 Application Security Gap Study: A Survey of IT Security & Developers*. Retrieved May 30, 2016, from http://www.ponemon.org/local/upload/file/2012_Application_security_gap_Final.pdf

Salancik, G. R., & Pfeffer, J. (1978). A Social Information Processing Approach to Job Attitudes and Task Design. *Administrative Science Quarterly*, 23(2), 224–253.

Settoon, R. P., Bennett, N., & Liden, R. C. (1996). Social Exchange in Organizations: Perceived Organizational Support, Leader–Member exchange, and Employee Reciprocity. Journal of Applied Psychology, 81(3), 219.

Symantec (2016). 2016 Internet Security Threat Report. Retrieved from https://www.symantec.com/security-center/threat-report

Thatcher, J., Liu, Y., Stepina, L., Goodman, J., & Treadway, D. (2006). IT Worker Turnover: An Empirical Examination of Intrinsic Motivation. ACM SIGMIS Database, 37(2–3), 133–146.

Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001). Embedding Security Practices in Contemporary Information Systems Development Approaches. *Info. Management & Computer Security*, 9(4)

Tøndel, I. A., Jaatun, M. G., & Meland, P. H. Akon. (2008). Security Requirements for the Rest of Us: A Survey. Software, *IEEE*, 25(1), 20–27.

Vallerand, R. J. (1997). Toward A Hierarchical Model of Intrinsic and Extrinsic Motivation. *Advances in Experimental Social Psychology*, 29, 271–360.

Van Eerde, W., & Thierry, H. (1996). Vroom's Expectancy Models and Work-Related Criteria: A Meta-Analysis. *Journal of Applied Psychology*, 81(5), 575.

Van Wyk, K. R., & McGraw, G. (2005). Bridging the Gap between Software Development and Information Security. *IEEE Security & Privacy*, 3(5), 75–79.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46(2), 186–204.

Vroom, V. H. (1964). Work and Motivation. New York, NY: John Willey & Sons.