6-18-2024

# Role of Human Resource Management in Information Security Compliance Behavior

Sahar Farshadkhah
*University of Illinois Springfield*, sfars2@uis.edu

Stephanie Maynard-Patrick
*University of Illinois Springfield*, smaynar2@uis.edu

# Role of Human Resource Management in Information Security Compliance Behavior

**Sahar Farshadkhah**
University of Illinois Springfield
sfars2@uis.edu

**Stephanie Maynard-Patrick**
University of Illinois Springfield
smaynar2@uis.edu

**ABSTRACT**

This paper aims to explore areas for practical and theoretical integration of information security and human resource domains based on the conducted findings from the focus group with Chief Information Security Officers and Chief Technology officers. It explores the idea that lack of organizational information security efforts from other departments hurts employee compliance. Responses from a focus group of executives have led us to explore potential points of integration with the firm's human resource department, a group tasked with orchestrating the firm's human capital to effectively work towards the firm's goals. It is our contention that information security departments can reduce employees' noncompliance behaviors by involving the HR department. HR-led work design interventions to limit job crafting and improving training can go beyond awareness and provide concrete steps for action.

**Keywords**

Information security compliance, job crafting, performance appraisal, job design, training, Human Resources.

## INTRODUCTION

Information security is an increasing problem that organizations are facing. Organizations need to consider different approaches to have a successful information security management. Ponemon Institute (2020) reported that the negligent insider is the root cause of most incidents. This shows the importance of employees' awareness about information security and their role in information security management of their organizations. To achieve higher employee awareness, organizations should invest in developing effective information security policies, employees' training, and auditing employees' security behaviors. However, the best organizational initiatives will not succeed if they are not supported by other departments and systems in the organization. One of the most far-reaching departments in an organization whose processes and systems affect every employee is the firm's human resource (HR) department. By working as a metaphorical island, information security departments miss out on additional levels of support and tools to use to increase organizational levels of employee information security compliance behavior (ISCB). This paper examines the ways HR can support information security goals including improved employee ISCB. In particular, it tackles two threats to employee ISCB, limiting job crafting and misaligned training and shows how HR department interventions can help facilitate ISCB.

In 2020 a focus group of Chief Information Security Officers (CISO) and Chief Technology officers (CTO) from organizations in South Florida was conducted. During the focus group, we explored how the executives set information security policies (ISPs). One executive shared: "When I need to create a new ISP, I simply sit down with my security team, and we outline what the policy should be. I write it and enter it into the system that holds all our (the firm's) policies and procedures." Follow up on this statement revealed that he and his team do not notify other departments of the change in policy made. All of the executives admitted they did not consult or partner with other departments beyond legal/risk management to ensure regulatory requirements were covered. When asked if non-IS/IT employees were involved in the policy and behavior development process, the answer was a resounding no across participants.

These comments made us question how information security (IS) working in isolation may result in the employee noncompliance behavior (Johnston & Warkentin, 2010). From a socio-technical systems approach, if the departments that are in charge of aligning people and technology are not communicating openly then there is little chance that the system is working at full efficiency. For instance, HR department plays a significant role in change management, organizational culture, and employee voice efforts and success in information security management should benefit from this in order to get better compliance behavior from employees.

This paper aims to explore areas for practical and theoretical integration of information security and human resource domains based on our findings from the focus group. Figure 1 models our propositions, theorizing that an integration of HR job analysis, design, and performance will limit the negative effects of employee job crafting on compliance behavior. The areas of job

design and evaluation and training and development, if integrated in information security management program, should increase employees' compliance with security policies.

## JOB ANALYSIS, DESIGN, AND EVALUATION

Theoretically, job crafting is an important construct that may help IS researchers understand and better predict employee compliance. Job crafting is "the actions employees take to shape, mold, and redefine their jobs" (Wrzesniewski & Dutton, 2001, p. 180). The increased use of job crafting by employees reflects the changing nature of work, which now requires flexibility, innovation, and changing solutions to novel problems. Coupled with employment trends like a shrinking workforce and rapid advances in technology, employees find they often have more to do than they feel capable of (D'Arcey et al., 2014). Job crafting is one of the ways that employees cope with perceived excess loads or the inability of resources, by selecting to reduce the number of tasks performed, called limiting job crafting (Wrzesniewski & Dutton, 2001). Unfortunately, this can result in employees eliminating tasks like information security policy compliance behaviors from their work when employees engage in job crafting.

**P1:** Employee limiting job crafting is negatively related to employee ISCB.

In order to prevent employees from choosing to remove information security-related vital tasks, information security teams can get help from HR to utilize the tools of job analysis, job design, and performance evaluation. Job analysis is the structured process of collecting data about what each job is required to do from managers, peers, incumbents, direct observation, and previous job holders in order for organizations to develop and maintain current job descriptions. Job analysis leads to the design (or redesign) jobs to include the tasks, responsibilities, and duties that will most effectively lead to achievement of the firm's goals (Noe et al., 2020). In addition, HR should be including in any new work requirements due to regulatory, technology, or process changes – such as information security compliance behaviors. However, if these behavioral requirements are not shared directly with HR, then HR may not include such topics in the employee's job description due to lack of awareness.

Performance appraisals are another tool that can be used to prevent removal of ISCB via job crafting and key employees into performing ISCB. If included in the formal performance appraisal criteria, managers and employees will understand the seriousness the firm gives information security. They will be more likely to follow the policies and perform the behaviors if failure to do so or have their subordinates do so would risk their compensation or chances for promotion. Therefore:

**P2:** HR interventions (job descriptions and performance appraisal) that integrate information security requirements will be positively related to employees actually performing ISCB.

**P3:** HR interventions (job descriptions and performance appraisal) that integrate information security requirements will fully mediate the relationship between limiting job crafting and employees ISCB.

### Training and Development

IS training is well established in organizations, as it aims to improve employees' awareness of information security and their efficacy beliefs about their ability to act securely (Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath & Rao, 2009). However, research has indicated that many organizations view IS training as a regulatory requirement that must be "checked off" in order for the firm to be in compliance with regulators (Damianides, 2005). Thus, employees may perceive IS training as a formality for employment and pay little attention to actually learning or implementing the material covered (Myyry et al., 2009; Glaspie & Karwowski, 2018). Despite this perspective, IS training has been considered a vital element to protecting information assets (Shaw et al., 2009).

**P4:** Information security training is positively related to employees ISCB.

Not all trainings are effective and must be carefully selected. For instance, a security training may train on topics other than what the organization needs employees to do. For instance, one CISO on the focus group shared the story of how he selected a phishing email training that explained very thoroughly what phishing emails were, how they worked, and what to do with emails so the new software being installed would handle the potential threat. The firm then ran a post-test by sending out phishing emails to see if fewer employees fell for the phishing scheme. The training only had marginal improvement of a few percent. Upon closer investigation with the employees, they learned that the employees' take away from the training was that the software would do everything, and the employees just needed to rely on the software. Thus, if the appropriate objectives (what the employees should have learned to do by the end of the training) and content (not just what to do but how to do it) are not included in the selected training then employees may not learn what the organization desires them to learn (Knowles et al., 1998). This content then must be aligned with the IS goals of the organization to ensure effectiveness (Ayyagari & Figueroa,

2017). Further, the message should align with the culture of the organization. HR department can help the IS/IT department by reviewing training options with IS to ensure alignment.

**P5:** Alignment between the training content, organizational IS goals, and organizational culture will moderate the relationship between IS training and ISCB in such a way that the greater the alignment, the greater effect training will have on compliance.

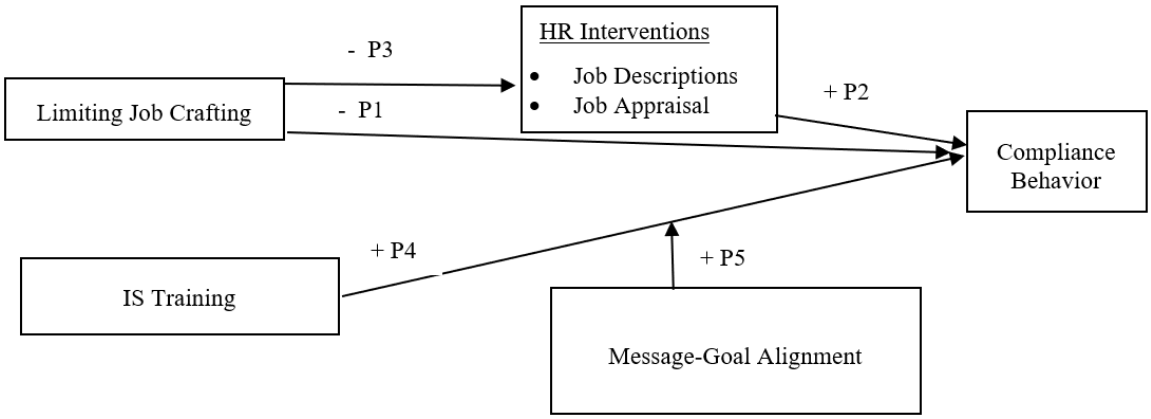


**Figure 1. Research model**

## CONCLUSION

It is important that individuals who are responsible in developing information security policies and roles be aware of the positive impact that HR could have in the process and take advantage of this asset in their organization. When there is a weak integration, firms are more likely to see a checklist compliance attitude and lack of accountability (e.g., that is not really my job). By cultivating a strong integration of human resource in which HR practices and systems are utilized to reach the organization's information security goals, organizations should see better employee compliance rates and fewer security incidents.

## REFERENCES

1. Ayyagari, R., and Figueroa, N. (2017) Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets, *Journal of Information Systems Education*, 28, 2, 115–121.
2. Bindl, U. K., Unsworth, K. L., Gibson, C. B., and Stride, C. B. (2019) Job Crafting Revisited: Implications of an Extended Framework for Active Changes at Work., *Journal of Applied Psychology*, 104, 5, 605–628.
3. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, 523-548.
4. D'Arcy, J., Herath, T., and Shoss, M. K. (2014) Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective, *Journal of Management Information Systems*, 31, 2, 285–318.
5. Damianides, M. (2005) Sarbanes–Oxley and It Governance: New Guidance on It Control and Compliance, *Information Systems Management*, 22, 1, 77–85.
6. Glaspie, H. W., and Karwowski, W. (2018) Human Factors in Information Security Culture: A Literature Review, in *Advances in Human Factors in Cybersecurity*, D. Nicholson (ed.), Cham: Springer International Publishing, 269–280.
7. Klein, H. J., Cooper, J. T., Molloy, J. C., & Swanson, J. A. (2014) The assessment of commitment: Advantages of a unidimensional, target-free approach, *Journal of Applied Psychology*, 99, 2, 222–238.
8. Leana, C., Appelbaum, E., and Shevchuk, I. (2009) Work process and quality of care in early childhood education: The role of job crafting. *Academy of Management Journal*, 52, 6, 1169–1192.
9. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009) What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study, *European Journal of Information Systems*, 18, 2, 126–139.
10. Noe, R., Hollenbeck, J., Gerhart, B., & Wright, P. (2020) Human Resource Management (12th ed.). McGraw Hill.

11. Ponemon Institute. (2020) Cost of Insider Threats: Global Report, Ponemon Institute. (https://www.ibm.com/downloads/cas/LQZ4RONE).
12. Shaw, R. S., Chen, C. C., Harris, A. L., and Huang, H.-J. (2009) The Impact of Information Richness on Information Security Awareness Training Effectiveness, *Computers & Education*, 52, 1, 92–100.
13. Wrzesniewski, A., and Dutton, J. E. (2001) Crafting a Job: Revisioning Employees as Active Crafters of Their Work, *Academy of Management Review*, 26, 2, 179–201.