Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2022 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-11-2022

A role theory perspective: Will shifting left become a pain for application developers?

Hwee-Joo Kam
University of Tampa

John D'Arcy
University of Delaware

Follow this and additional works at: https://aisel.aisnet.org/wisp2022

Recommended Citation

Kam, Hwee-Joo and D'Arcy, John, "A role theory perspective: Will shifting left become a pain for application developers?" (2022). *WISP 2022 Proceedings*. 12.
https://aisel.aisnet.org/wisp2022/12

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A Role Theory Perspective: Will Shifting Left Become a Pain for Application Developers?

Hwee-Joo Kam
Sykes College of Business, University of Tampa
Tampa, FL, USA

John D'Arcy
Lerner Business and Economics, University of Delaware
Newark, DE, USA

ABSTRACT

To foster application security (AppSec), organizations are adopting development, security, and operations (DevSecOps) framework that integrates application development with security controls and systems operations. With DevSecOps. application developers have to "wear many hats". Besides coding, developers are assigned additional tasks including system testing and operations, thus adopting the roles of systems testers and systems engineers. Transitioning from one role to another involves boundary crossing through which individuals have to embrace changes for performing new tasks defined by another role. This may instigate developers' mental fatigue. Also, tasks associated with "non-developer" roles (e.g., systems operations) may not be a good cognitive fit, thus provoking developers' mental distress. To address this issue, we examine the effects of multi-roles adoptions on developers' well-being that will gradually affect their cognitions of cyber situational awareness (i.e., awareness of cyber threats relative to AppSec).

Keywords: application security, situational awareness, role theory, DevSecOps, developers

INTRODUCTION

Application security (AppSec) vulnerabilities have been threatening organizations' information security (InfoSec) (Yasasin et al. 2020). The 2021 Verizon Data Breach Investigations Report (DBIR) revealed that exploitation of web *application* vulnerabilities was responsible for more than 20% of data breaches (Verizon 2021). There is a difference between software and application (Kravchuk 2021). Software executes system-level and application-level

operations through interactivities between a set of programs and operating systems, whereas application is mostly designed to solve business problems (Kravchuk 2021). This study uses the term *applications* to denote digital solutions that facilitate business operations.

For vulnerabilities mitigation, organizations "shifted left" to embrace Development, Security, and Operations (DevSecOps) framework (GitLab 2022) that integrates systems operations (e.g., configuration) and InfoSec (e.g., security testing) into application development. With DevSecOps, organizations shifted the responsibilities of AppSec safeguards to application developers, compelling developers to "wear many hats". The GitLab 2022 Global DevSecOps Survey revealed that 38% of the surveyed developers were assigned additional tasks such as monitoring the operations of applications in an information technology (IT) platform (GitLab 2022). Developers are taking on the roles of system engineers (i.e., system operations) and system testers (i.e., security testing). Based on the same survey, Silverthorne (2022) stated:

> *"Today's developers are literally DIYing all the [operations] things. This year, 38% reported instrumenting code they've written for production monitoring, up 12% from 2021 and more than double the percentage in 2020."* (Silverthorne 2022)

A role pertains to a position with specified responsibilities (Ashforth et al. 2000). When developers switch from developing an application (i.e., coding) to monitoring that application's operations, developers have to disengage from coding that embodies syntactic knowledge processing (i.e., programming) (Bishop-Clark 1995) and creative problem-solving (Graziotin et al. 2014); and next adopt systems engineering tasks that demand system configurations via systematic processing and via conceptualization of interrelatedness between system components (Kam and Shang 2019). Such a transition could cause mental fatigue, as disengaging from a current role and adopting another would trigger mental exhaustion (Ashforth et al. 2000).

Furthermore, tasks associated with systems engineering are usually beyond developers' craft. Trained for application development, developers may find it hard to conceptualize systems complexities built on diverse networks of system components. Although many developers have built applications distributed across multiple IT systems, such development is quite different from managing diverse network systems that spanned through different network architectures and boundaries. This suggests that systems engineering's tasks may not be a good cognitive fit for developers (Chilton et al. 2005), possibly because developers gained job satisfaction through creative problem-solving (Gallivan 2003) rather than through handling system complexities.

We also assert that, besides code quality and productivity (Weeks and Schleen 2020), developers' well-being is critical to cyber situational awareness (SA). Built on Endsley's (1988) notion of SA, we argue that cyber SA subsumes individuals' perceptions of cyber environments and individuals' projections of cyber threats relative to AppSec assurance. Since human's efforts are critical to SA (Barford et al. 2010) that is cognitively demanding (Franke and Brynielsson 2014), developers' deteriorated well-being resulted from multi-role transitions would undermine their cyber SA. To address this concern, we form the following research questions:

R1: In an application security context, how would multi-roles transitions affect application developers' well-being?

R2: How would application developers' well-being affect their cyber situational awareness?

This study contributes to the information systems (IS) research by addressing an up-to-date topic related to AppSec. The criticality of AppSec has been well recognized, but not the actors (i.e., application developers) who have great influence on AppSec. To fill in the research gap, our research findings will provide insights regarding one of the factors (i.e., developers' cyber SA based on role transitions) that may influence AppSec through the lens of DevSecOps.

LITERATURE REVIEW

Development, Security, and Operations

With development, security, and operations (DevSecOps), application developers have to wear many hats for performing tasks such as systems engineering (e.g., monitoring applications' operations) and security testing (e.g., running AppSec tests) (GitLab 2022). Since DevSecOps promotes "shifting left", collaborative efforts among developer, security, and operation teams start early in the application development life cycle (Myrbakken and Colomo-Palacios 2017).

DevSecOps demands speed and agility (Callanan and Spillane 2016). This suggests that not only developers have to be effective in continuous processes involving continuous integration (CI) (e.g., automatically run error-checking on codes and integrate codes written by multiple developers) and continuous delivery (CD) (e.g., deploying new applications to a production environment) (Humble and Molesky 2011), but they have to also actively participate in continuous testing (i.e., automating testing in each development phase to detect anomaly) and monitoring (i.e., regularly produce evidence to show that an application is functioning in each development phase) (Myrbakken and Colomo-Palacios 2017). Thus, application developers have to shoulder many responsibilities in their day-to-day tasks. Although automation may ease some of the developers' burdens, developers working in organizations with less resources are often swamped with work. High job demands created by DevSecOps will eventually provoke burnout (Bakker et al. 2004) that would harm developers' well-being (Benlian 2022).

Role Transitioning Theory

Developers' well-being might also be affected by role transitioning. Role transitions entail psychological movements that disengage from one role and engage in another (Richter 1984). Because application developers regularly switch between roles of developers, security

testers, and system engineers, such role transitions are frequent and do not have to overcome physical boundaries (i.e., geographical constraints). This indicates that micro role transitions occur (Ashforth et al. 2000). A role denotes a position defined with a set of responsibilities, thus suggesting that a role boundary defines the scope of a given role (Ashforth et al. 2000).

Micro role transitions are affected by flexibility and permeability of a role boundary (Ashforth et al. 2000). Flexibility refers to the degree of pliability of spatial and temporal boundaries (Hall and Richter 1988), whereas permeability refers to the degree of role multitasking in which one could physically located at a role's domain and psychologically engaged in another role (Pleck 1977). Because application developers can easily switch to systems engineers or systems testers without immense spatial and temporal constraints, we assert that developers' role transitioning involve high flexibility and permeability.

Alternatively, micro role transition is affected by role identity -- a social construct shaped by core and peripheral features (Ashforth et al. 2000). Core features exemplify the main characteristics of a role, while peripheral features signify "secondary" attributes. For example, the core features that shape a developer role could be logical thinking, creative problem-solving, and team player, whereas the peripheral features could be managerial skills. Difficulty in role transitions may stem from the contrast of core and peripheral features between a pair of roles (Ashforth et al. 2000). That is, role transition is affected by the magnitude of changes involved to acquire the skills in the prescribed features of a different role (Ibarra and Barbulescu 2010).

Application developers changing from a developer role to a systems engineer role have to switch from divergent thinking (i.e., creative thinking that involves thinking outside the box) (Bishop-Clark 1995; Gallivan 2003) to convergent thinking (i.e., a thought process that integrates interrelated components) (McCumber and Sloan 2002). This is mainly because

application development embodies divergent thinking, in which a solution is derived from a flexible approach of thinking that diverges from the problem on hand (i.e., thinking outside the box) (Bishop-Clark 1995). Conversely, systems engineering espouses convergent thinking through which an integrative approach connects interrelated components to facilitate system functionalities (McCumber and Sloan 2002). In this context, switching cognitive gear (i.e. from divergent to convergent cognitions) could trigger mental fatigue (Louis and Sutton 1991). While some may find it cognitively "fun" to switch between both thinking modes, many developers are working under immense time pressure (Austin 2001) so any additional cognitive demand would jeopardize their job performance and well-being (Benlian 2022; Graziotin et al. 2014).

Cyber Situational Awareness

In addition to juggling different roles, application developers must maintain cyber situational awareness (SA). Overall, SA embodies individuals' perceptions and projections of a given environment within the boundary of time and space (Endsley 1988). Based upon this notion, we contend that cyber SA subsumes individuals' perceptions of and comprehensions on cyber environments, and individuals' projections of cyber threats in relation to AppSec assurance. Alternatively, cyber SA denotes individuals' cognitive capacity of making good judgement based on their understanding of technology complexities (Zhong et al. 2018).

While numerous studies discussed cyber SA from IT (D'Amico et al. 2005; Jajodia and Albanese 2017; Zhong et al. 2018) and management (Ahmad et al. 2019, 2021) perspectives, we assert that it is also important to address cyber SA on behalf of application developers. Human plays an important role in maintaining cyber SA (Barford et al. 2010). Developers who are aware of and understand how cyber threats could exploit application vulnerabilities would be more vigilant in implementing AppSec design (Assal and Chiasson 2019). Hence, we address

cyber SA to examine developers' awareness of cyber threats and their understanding of how these threats would exploit vulnerabilities of the applications that they develop.

CONCLUSION AND FUTURE RESEARCH

In conclusion, this study investigates how the dynamic of DevSecOps would affect application developers' well-being ascribed to their Cyber SA. This study will contribute to IS research in the following ways. First, while the IS research community emphasized the importance of DevOps (Maruping and Matook 2020), we went one step further to investigate developers' well-being in a DevSecOps context. That is, we integrate InfoSec and system engineering into application development to study developers' behaviors. Second, to the best of our knowledge, there are not many studies that examine cyber SA among application developers who develop applications that will always be explored and likely be exploited by cyber threats. Therefore, our research findings will provide insights on how developers maintain SA to foster AppSec assurance. We believe that these insights will help improve AppSec. Finally, in the near future, we will interview application developers who are participating in DevSecOps. We will also design semi-structured questions and use context analysis (Weber 1990) to analyze data.

REFERENCES

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., and Baskerville, R. L. 2021. "How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice," *Computers & Security* (101), p. 102122.

Ahmad, A., Webb, J., Desouza, K. C., and Boorman, J. 2019. "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," *Computers & Security* (86), pp. 402–418.

Ashforth, B. E., Kreiner, G. E., and Fugate, M. 2000. "All in a Day's Work: Boundaries and Micro Role Transitions," *The Academy of Management Review* (25:3), Academy of Management, pp. 472–491. (https://doi.org/10.2307/259305).

Assal, H., and Chiasson, S. 2019. "'Think Secure from the Beginning': A Survey with Software Developers," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, New York, NY, USA: Association for Computing Machinery, May 2, pp. 1–13. (https://doi.org/10.1145/3290605.3300519).

Austin, R. D. 2001. "The Effects of Time Pressure on Quality in Software Development: An Agency Model," *Information Systems Research* (12:2), INFORMS, pp. 195–207.

Bakker, A. B., Demerouti, E., and Verbeke, W. 2004. "Using the Job Demands-Resources Model to Predict Burnout and Performance," *Human Resource Management* (43:1), pp. 83–104.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., and Yen, J. 2010. "Cyber SA: Situational Awareness for Cyber Defense," in *Cyber Situational Awareness: Issues and Research*, Advances in Information Security, S. Jajodia, P. Liu, V. Swarup, and C. Wang (eds.), Boston, MA: Springer US, pp. 3–13. (https://doi.org/10.1007/978-1-4419-0140-8_1).

Benlian, A. 2022. "Sprint Zeal or Sprint Fatigue? The Benefits and Burdens of Agile ISD Practices Use for Developer Well-Being," *Information Systems Research* (33:2), INFORMS, pp. 557–578. (https://doi.org/10.1287/isre.2021.1069).

Bishop-Clark, C. 1995. "Cognitive Style, Personality, and Computer Programming," *Computers in Human Behavior* (11:2), pp. 241–260.

Callanan, M., and Spillane, A. 2016. "DevOps: Making It Easy to Do the Right Thing," *IEEE Software* (33:3), pp. 53–59. (https://doi.org/10.1109/MS.2016.66).

Chilton, M. A., Hardgrave, B. C., and Armstrong, D. J. 2005. "Person-Job Cognitive Style Fit for Software Developers: The Effect on Strain and Performance," *Journal of Management Information Systems* (22:2), Routledge, pp. 193–226. (https://doi.org/10.1080/07421222.2005.11045849).

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., and Roth, E. 2005. "Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (49:3), SAGE Publications Inc, pp. 229–233.

Endsley, M. R. 1988. "Design and Evaluation for Situation Awareness Enhancement," *Proceedings of the Human Factors Society Annual Meeting* (32:2), SAGE Publications, pp. 97–101. (https://doi.org/10.1177/154193128803200221).

Franke, U., and Brynielsson, J. 2014. "Cyber Situational Awareness – A Systematic Review of the Literature," *Computers & Security* (46), pp. 18–31. (https://doi.org/10.1016/j.cose.2014.06.008).

Gallivan, M. J. 2003. "The Influence of Software Developers' Creative Style on Their Attitudes to and Assimilation of a Software Process Innovation," *Information & Management* (40:5), pp. 443–465. (https://doi.org/10.1016/S0378-7206(02)00039-3).

GitLab. 2022. "The GitLab 2022 Global DevSecOps Survey," Thriving in an Insecure World, GitLab. (https://about.gitlab.com/developer-survey/#developers).

Graziotin, D., Wang, X., and Abrahamsson, P. 2014. "Happy Software Developers Solve Problems Better: Psychological Measurements in Empirical Software Engineering," *PeerJ* (2), PeerJ Inc., p. e289. (https://doi.org/10.7717/peerj.289).

Hall, D. T., and Richter, J. 1988. "Balancing Work Life and Home Life: What Can Organizations Do to Help?," *Academy of Management Perspectives* (2:3), Academy of Management, pp. 213–223. (https://doi.org/10.5465/ame.1988.4277258).

Humble, J., and Molesky, J. 2011. "Why Enterprises Must Adopt Devops to Enable Continuous Delivery," *Cutter IT Journal* (24:8), p. 6.

Ibarra, H., and Barbulescu, R. 2010. "Identity as Narrative: Prevalence, Effectiveness, and Consequences of Narrative Identity Work in Macro Work Role Transitions," *The Academy of Management Review* (35:1), Academy of Management, pp. 135–154.

Jajodia, S., and Albanese, M. 2017. "An Integrated Framework for Cyber Situation Awareness," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 29–46.

Kam, H.-J., and Shang, Y. 2019. "Improving Cybersecurity Learning: An Integration of Cyber Offense and Cyber Defense," in *PACIS 2019 Proceedings*, Xi'an, China, June 15. (https://aisel.aisnet.org/pacis2019/177).

Kravchuk, I. 2021. "Learn the Difference Between Software vs Application," , May 19. (https://tateeda.com/blog/difference-between-software-vs-application, accessed June 27, 2021).

Louis, M. R., and Sutton, R. I. 1991. "Switching Cognitive Gears: From Habits of Mind to Active Thinking," *Human Relations* (44:1), SAGE Publications Ltd, pp. 55–76. (https://doi.org/10.1177/001872679104400104).

Maruping, L. M., and Matook, S. 2020. "The Evolution of Software Development Orchestration: Current State and an Agenda for Future Research," *European Journal of Information Systems* (29:5), Taylor & Francis, pp. 443–457. (https://doi.org/10.1080/0960085X.2020.1831834).

McCumber, W. H., and Sloan, C. 2002. "Educating Systems Engineers: Encouraging Divergent Thinking," *INCOSE International Symposium* (12:1), pp. 8–15. (https://doi.org/10.1002/j.2334-5837.2002.tb02436.x).

Myrbakken, H., and Colomo-Palacios, R. 2017. "DevSecOps: A Multivocal Literature Review," in *Software Process Improvement and Capability Determination*, Communications in Computer and Information Science, A. Mas, A. Mesquida, R. V. O'Connor, T. Rout, and A. Dorling (eds.), Cham: Springer International Publishing, pp. 17–29. (https://doi.org/10.1007/978-3-319-67383-7_2).

Pleck, J. H. 1977. "The Work-Family Role System*," *Social Problems* (24:4), pp. 417–427. (https://doi.org/10.2307/800135).

Richter, J. 1984. *The Daily Transition between Professional and Private Life*, Boston, MA: Boston University.

Silverthorne, V. 2022. "Why - and How - DevOps Roles Are Changing," *GitLab*, , August 31. (https://about.gitlab.com/blog/2022/08/31/the-changing-roles-in-devsecops/, accessed October 2, 2022).

Verizon. 2021. "2021 Data Breach Investigations Report (DBIR)," Verizon Enterprise. (https://www.verizon.com/business/resources/reports/dbir/).

Weber, R. P. 1990. *Basic Content Analysis*, Newbury Park, CA: SAGE.

Weeks, D., and Schleen, D. J. 2020. "7th Annual DevSecOps Community Survey," Sonatype.

Yasasin, E., Prester, J., Wagner, G., and Schryen, G. 2020. "Forecasting IT Security Vulnerabilities – An Empirical Analysis," *Computers & Security* (88), p. 101610.

Zhong, C., Lin, T., Liu, P., Yen, J., and Chen, K. 2018. "A Cyber Security Data Triage Operation Retrieval System," *Computers & Security* (76), pp. 12–31. (https://doi.org/10.1016/j.cose.2018.02.011).