THE UNIVERSITY OF TAMPA

Influence of Outside Adversities on DevSecOps work Practices: Socio-Technical Perspective

Avi Jain (Masters of Science – Cybersecurity)

Faculty Mentor- Muhammad Al-Abdullah (Information and Technology Management) - Sykes College of Business: University of Tampa

MOTIVATION

- The research motivation is to study the influence of outside adversities on DevSecOps work practices from a socio-technical perspective.

From Research Perspective:

DevSecOps has been studied only from a technical perspective.

- Teams they work with
- Technology they use and have available their skills in using technology
- Environment they work within
- Business objectives
- Implementation of security measures

From Socio-Technical:

- Allow understanding those influences to enhance their productivity in takin off any obstacles in their way.

Contribution to Practical Perspective,

- Understand DevSecOps work environment
- Recommendations of the factors to build the most efficient work practices for DevSecOps.

PURPOSE OF THE STUDY

- The purpose of the study was to understand the importance of DevSecOps by implementing the Security by Design with the Development and Operations.
- Keeping in mind the current problems in the area, some of them are as follows:

1.) Limited access to Technology-

- Lack of tools or technology solutions
- Limited support of automate security testing and monitoring
- Slower development cycles
- Lack of visibility into security vulnerabilities.

Importance of DevSecOps:

- Framework for integrating security into every stage of the development lifecycle.
- Enabling organizations to identify and remediate security issues early on.
- Improving their overall security posture
- Maintaining agility and innovation.

2.) Security in coding is an ad-hoc due to lack of Awareness-

- Security is rarely integrated as a core part of the development process
- Leads to vulnerabilities introduced into the final product as a result
- Less awarness among developers about the importance of security

Importance of DevSecOps:

- Integrate security into every stage of the development lifecycle
- Help developers understand the importance of security
- Identify vulnerabilities early on
- Create a culture of security across the organization

3.) Fixing the problems at the later stages-

- Costly
- Time consuming
- Non-alignable with the goal of the final product
- Causes to redo everything, sometimes not doable.

Importance of DevSecOps:

- Automation and monitoring
- Help teams identify and remediate security issues discovered in the later stages
- Reduces the cost and time required to fix security issues
- Prevent the need to redo everything from scratch.

4.) Understanding between different departments-

- Difficult to work together as a team
- Challenging for different teams involved in the software development process
- Difficulties in integrating security into their workflows

Importance of DevSecOps:

- Creates a shared understanding of security across different departments
- Provides real-time feedback on security issues
- Fosters collaboration by reducing the risk of misunderstandings or conflicting priorities.

5.) Management is not supportive-

- Challenging to get support from upper management
- A shift can require changes to organizational structures, processes, and culture.

Importance of DevSecOps:

- Reduce the cost of security incidents
- Avoid reputation damage
- Reduce the time and resources required to address security issues
- Adopt a culture of continuous improvement

6.) Outside influence-

- Manage risks originating from outside adversities
- NO direct control of the development team.

Importance of DevSecOps:

- Include risk assessment methodologies that identify and address security risks
- Continuous monitoring can help detect and address security risks

7.)Resistance to change-

- Getting people and organizations to adopt new ways of working

Importance of DevSecOps:

- Embrace the cultural changes that emphasize outcomes over outputs
- Focus on delivering value to customers
- Create a culture that is more focused on results
- Culture less resistant to change

8.) Compliance and Regulatory requirements-

- Use of specific security measures
- May place limitations on how data can be processed and stored.

Importance of DevSecOps:

- Automated compliance checks that can be built into the software development pipeline
- Ensure that software meets regulatory requirements without requiring manual checks or audits.

9.) Cloud security-

- Migration of applications and data to the cloud
- Protection of data at rest, data in transit and data in use

Importance of DevSecOps:

- Infrastructure as code
- Uses a high-level programming language rather than manually configuring individual resources
- Ensures the security of cloud resources and applications

DATA/RESEARCH METHOD

- We are conducting a systematic literature review.

Research Questions

- What interventions are used to align the technical and social environments for DevSecOps?
- How do systems outside the organizational boundary influence DevSecOps work practices?
- How do successful DevSecOps environment manage individual and/or team resistance to change?

Filter Process steps	Results
Identify Articles	50
Remove Duplicates	27
Screen Abstract	23
Screen Full text	18

Journal	Number of Papers
Proceedings of the 21st European Conference on Cyber Warfare and Security	1
Wiley Publications	1
Conference Paper- ResearchGate	1
30th Annual INCOSE International Symposium	1
Future Internet 2022-MDPI	1
Organization Studies 28(09): 1435–1448 ISSN 0170–8406	1
Arvix.org	1
Chinese Academy of Engineering and Higher Education Press	1
Intelligent Systems, IEEE	1
2021 The Institution of Engineering and Technology	1
Secure Systems and Smart Card Group, IBM Thomas J. Watson Research Center, Hawthorne, NY	1
Signal Processing for Next Generation Wireless Networks	1
Information Technology & People	1
Information and Software Technology- Creative Commons	1
IEEE Xplore	1
International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012	1
Scielo.org.co	1
2011 11th International Conference on Quality Software	1

About DevSecOps:

- DecSecOps framework are required to include security in the software development to build a cybersecurity aware environment within an organization.

Challenges:

- Lack of awareness about the importance of security in coding
- Cost and time required to fix problems at later stages of development
- Difficulties in getting teams to work together
- Lack of support from management
- External influence from third-party components and cloud providers

Solutions:

- Involve all stakeholders in the process
- Communicate the benefits of DevSecOps
- Create a culture of experimentation
- Continuous improvement to encourage people to embrace change
- Improve the overall security posture of their software products

RESULTS

Based on the Literature review we found that the Socio-Technical framework needs to be implemented for effective DevSecOps practices:

- Cross-functional Collaboration
- Agile and Lean Principles
- Automation and Tooling
- Training and Skill Development
- Leadership and Change Management
- Shared Metrics and KPIs
- Security Requirements

- Threat Modeling
- Security Testing
- Compliance Requirements
- Change Management
- Communicate the Benefits
- Provide Education and Training
- Foster Collaboration and Inclusion
- Address Concerns and Provide Support
- Lead by Example
- Monitor and Adjust
- Recognize and Celebrate Successes

- Hence, a maturity model that implements these above-mentioned factors are required.

CONCLUSION

- The purpose of studying the influence of outside adversities on DevSecOps work practices from a Socio-Technical Perspective is to provide insights into how organizations can better manage these risks to improve the security and functionality of their software systems.

- By identifying best practices for managing cyber security risks, securing physical infrastructure, and managing user access and privileges, organizations can improve their software security, enhance their software functionality, and increase user trust.
- The potential results of this study can be practical, such as the identification and analysis of outside adversities, or theoretical, such as the development of more effective DevSecOps practices.

BIBLIOGRAPHY

Naidoo, R., & Möller, N. (2022, June). Building Software Applications Securely With DevSecOps: A Socio-Technical Perspective. In *ECCWS 2022 21st European Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited.

Carey, M. J., & Jin, J. (2019). *Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity*. John Wiley & Sons.

Mallouli, W., Cavalli, A. R., Bagnato, A., & De Oca, E. M. (2020, July). Metrics-driven DevSecOps. In *ICSOFT* (pp. 228-233).

Andersson, R., & Edström, C. (2022). Integrating security into agile software development: A case study on the role of inertia.

Dove, R., & Willett, K. D. (2020, July). Contextually aware agile security in the future of systems engineering. In *INCOSE International Symposium* (Vol. 30, No. 1, pp. 1501-1516).

Almeida, F., Simões, J., & Lopes, S. (2022). Exploring the benefits of combining DevOps and agile. *Future Internet*, *14*(2), 63.

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organization studies*, *28*(9), 1435-1448.

Yilma, B. A., Panetto, H., & Naudet, Y. (2021). Systemic formalisation of Cyber-Physical-Social System (CPSS): A systematic literature review. *Computers in Industry*, *129*, 103458.