Chapter 117

Agile Principles in Responding to Safety Incidents in Productive Systems: a Systematic Review

10.56238/tfisdwv1-117

Rodrigo Sotolani
Rodrigo Silva Sotolani - ORCID id https://orcid.org/0000-0001-8729-8142 - Ci enter State Of Technological Education Paula Souza – CEETPS
E-mail: rodrigo.sotolani@cpspos.sp.gov.br

Napoleon Galegale
Napoleon Verardi Galegale - ORCID id https://orcid.org/0000-0003-2228-9151 - CState University of Technological Education Paula Souza – CEETPS
E-mail: nvg@galegale.com.br

ABSTRACT

Production systems have been integrated into the digital scenario where everything is connected, driven by Industry 4.0. In this complex, and heterogeneous and interconnected environment, it is necessary to observe the pillars of information security: integrity, confidentiality and availability. To answer to information security incidents, governments and organizations maintain CSIRTs, acronym for Computer Security Incident Response Teams, which manage incidents through processes to detect, analyze, respond and learn from incidents. However, these incident response teams generally follow a rigid and hierarchical structure, indicating problems in their processes. The agile approach has been considered a good option for solving these problems since agile principles have been used in areas outside of software development and also for addressing solutions that are not very clear at the beginning, for focusing on people, on constant feedback and acceptance of constant changes The present paper aims to carry out a systematic review of the literature located in the field of response to security incidents in production systems, in addition to agile principles and values. Thus, the research question of this article "What results are found in the literature on the use of agile principles in information security incident response processes in production systems?", resulted in six articles that address the use of agile principles in responding to information security incidents. Thus, the survey demonstrated a gap in the use of agile principles in responding to information security incidents. The result contributes demonstrating the need for further research on the use of agile principles in information security. It is envisioned that this area may have greater contributions during future research.

Keywords: Agile Principle, Incident Response, Information Security, Cyber Security, Productive Systems.

1 INTRODUCTION

Leveraged by Industry 4.0, production systems have integrated into the digital landscape where everything is interconnected. Through a virtual representation at a higher level of automation, many systems and software can communicate from the factory with the latest trends in information and communication technologies, reaching all elements of the value production chain in a real-time engagement.(ALCÁCER; CRUZ-MACHADO, 2019)

Technological advances in production systems create and treat valuable information that needs to be protected for the industrial success and safety of the entire system. In a complex, heterogeneous and interconnected environment, it is necessary to observe the premises of integrity, confidentiality and availability, pillars of information security.

The exponential growth of Internet interconnections has led to a significant growth in cyberattack incidents, often with disastrous and serious consequences. Second Liu et al. (2019) lyModarresi and Symons (2020), with the widespread adoption of Internet of Things (IoT) technologies, the surface of cyber-attacks has increased dramatically and has spread, giving new mechanisms for intrusionand potentialfor catastrophic damage to the privacy, security and protection of individuals and corporations.

In a successful cyberattack, the victims would not only be commercial organizations with financial losses, but also the population across the country. Failure of systems integrated with critical industries can lead to environmental disasters and fatal accidents.(PAVLENKO, 2019)

Most devices connectedto Cyber-Physical Systems (CPS) have long service life and many of them do not receive sufficient security updates or are never upgraded, resulting in attacks that can have serious consequences on human lives, business productivity, and national security.(WALKER-ROBERTS et al., 2020)

The management of information security in organizations and agility in responding to internal and external information security incidents could provide greater competitiveness, risk reduction, increased performance in companies.

To respond to information security incidents and initially motivated by *the US Defense Advanced Research Projects Agency* (DARPA), governments and organizations maintain the CSIRT's, acronym for *Computer Security Incident Response Teams*, that is, information security incident response group. CSIRTs manage security incidents through processes to detect, analyze, respond to, and learn from incidents that threaten the confidentiality, availability, and integrity of data and critical systems. .(RUEFLE et al., 2014)(RUEFLE et al., 2014)

A second information security incident is defined as a breach or imminent threat of violation of security policies, usage policies, or standard security practices. According to , information has strategic importance, is driven with the use of Information Technology (IT) in organizational processes and must have adequate protection.(CICHONSKI et al., 2012)Galegale, Fontes and Galegale (2017)

Today's CSIRTs use defined policies, procedures, and guides to help create consistent, quality-oriented, and repeatable processes. However, they highlight that this linear action plan approach presents(RUEFLE et al., 2014)Grispos et al. (2014)some problems, such as: (1) Lack of efficiency to deal with and manage incidents; (2) Interruption of the investigation by not completing a stage of the process; (3) Excessive focus on containment, eradication and recovery; (4) Lack of clarity to the root causes of the incident; (5) Poor planning; (6) Do not maximise the benefits of digital forensics; (7) Weakening the value of forensic evidence. There is still negligence in the use of lessons learned from incidents and post-incident functions.Ahmad et al. (2012)

These rigid and procedural incident response processes are increasing the predictability of defense efforts and make it more difficult to protect remaining infrastructure and business functions in the context of fast, multi-faceted cyber attacks(SMITH et al., 2021) .

The agile approach has been consideradto an option for solving traditional incident response problems since agile principles have been used in areas outside of software development such as consulting, manufacturing, *coaching* and also for meeting the solutions are not very clear at first, for focusing on people, on constant feedbacks and on the acceptance of constant changes. According to , collaboration in teams was higher when agile methods were adopted.(AMORIM et al., 2018)Stefani and Feitosa (2019)

Thus, the research question of this article is "What results are found in the literature on the use of agile principles in the processes of response to information security incidents of productive systems?".

The aim of this article is to conduct a systematic review study on scientific article databases to identify the works that deal with the agile approach in the processes of response to information security incidents.

The sequence of this article presents the theoretical framework in Section 2; the method used for the development of the study in Section 3; Section 4 presents the results and discussions regarding the documents collected; and finally in Section 5, the final considerations.

2 THEORETICAL FRAMEWORK

In this section will be addressed in a brief theoretical framework in the researched literature on agile practices applied outside the area of *software development* and the use of agile principles in responding to information security incidents.

2.1 AGILE PRACTICES BEYOND *SOFTWARE DEVELOPMENT*

Agile processes and practices are characterized by their underlying values and principles. Its use brought solution to the (BECK et al., 2001; FOWLER; HIGHSMITH, 2001)*software crisis*, solving the problem of requirements elaboration, changes and *software improvements*, bringing developers and owners closer to the products. It was possible to perform the implementation in an itenative and incremental way, adding value to the product through continuous improvements.

After a period of increased success rates in *software development*, *improved quality* and speed, and encouraged motivation and productivity of IT teams, agile methods are spreading across a wide range of industries and functions and even in senior management. For example, we mention: production of agricultural machinery, production of new fighter jets, marketing, human resources and even wine production.(RIGBY; SUTHERLAND; TAKEUCHI, 2016)

The hybrid use of agile methods with traditional methods was suggested by COOPER & SOMMER (2016) integrating the agile approach to the *Stage-Gate method* in order to achieve potential benefits for manufacturers of B2B physical products. It was also used Amorim et al. (2018) by to manage the implementation of IT governance with COBIT 5, called *Water-Scrum-Fall*, which aimed to overcome challenges such as the lack of support from senior management and the misalignment of scopes and solutions.

2.2 AGILE PRINCIPLES IN RESPONDING TO INFORMATION SECURITY INCIDENTS

Agile practices and principles could help solve the challenges of the traditional processes of a CSIRT, which are exposed Grispos, Glisson and Storer (2014)by , the processes do not reflect the dynamism of today's world, are slow and are not appropriate to the highly collaborative nature of these teams.

A *framework* to improve incident response processes in Sistemas de Controle Industrial (ICS) applying the benefits of agile values and practices was proposed by He and Janicke (2015). From the managerial perspective, the authors relate the unique characteristics of sHF with agile values, mentioning availability as the main concern.

For the current monitoring of incidents and Shedden et al. (2010)*post-mortem activities represent* a critical phase in the process. The authors point out the application of double *loop* learning to question fundamental processes and principles, a similar form to the S *CRUM retrospective*.

The technical report of , gives perspective to the social skills of a CSIRT, which meets the theme investigated in this research. The work environment of the CSIRTs involves collective activities between different profiles of professionals and resemblethe VUCA typePfleeger (2017), acronym *for volatile*, uncertain, *complex* and *ambiguous*, a way very close to agile principles. The author identified several processes and social dynamics that contribute to a more effective incident response.

Addressing the theme about the incident response process, the authors highlight its final phase: Grispos, Glisson and Storer (2017)*feedback*/follow-up. They bring organizations to find it difficult to learn from incidents and investigate the integration of agile and meta-retrospective light retrospectives into the security incident response process to improve *feedback and follow-up efforts*.

Naseer et al. (2021) argue that (1) organizations must develop agility in their incident response process to act quickly and efficiently to sophisticated and powerful cyber threats, and that (2) real-time analytics gives organizations a unique opportunity to conduct their incident response process in an agile manner, quickly detecting cybersecurity incidents and responding to them proactively.

Traditional incident response teams often follow a rigid, hierarchical structure. Individuals are assigned to a specialized function, such as *firewalls*, threat hunting, among others. This segregation of tasks often leads to the creation of information and knowledge silos, where attempts to pass information and skills to other relevant units can be suboptimal.(SMITH et al., 2021)

There is empirical evidence that *playbooks*, that is, the standard static incident response procedures generally adopted, do not offer sufficient flexibility to support situations outside their initial scope and that were ignored when the incidents occurred. A thematic analysis of semi-structured interviews with ICS incident response professionals identified three main areas of concern: communication, information sharing between areas of knowledge and obtaining external support.(SMITH et al., 2021)

Smith et al. (2021)propose that agile principles aim to break the silos of information and knowledge by creating more integrated teams and to do so, list only three distinct functions within a team: incident owner, *SCRUM master* and team member, creating for this a framework called AIR4ICS, acronym *for Agile Incident Response For Industrial Control Systems* , giving new meaning to agile practices applied in information security.

3 METHOD

The methodology of this study, according to Prodanov & de Freitas (2013), can be classified as nature as a basic research. As for the objective, as exploratory and descriptive research. And as for the scientific procedure, systematic review.

The literature review used the SCOPUS database for its coverage of areas of scientific knowledge and integrate with computational tools that assist in the recovery of metadata.

The findings were analyzed quantitatively and qualitatively with the prisma-p (*Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols*) research protocol, aiming at a systematic review and a pre-planned methodological and analytical approach. The use of this protocol was motivated to ensure the quality of the research and also to achieve the reliability and validity of the results through the qualitative evaluation of the selected scientific articles.

Data were collected in September 2021, with the keywords used: "*agile principles*", *"security incident response" and* variations "*agile method", "security incident handling"*. Theydo not apply tos date limitations.

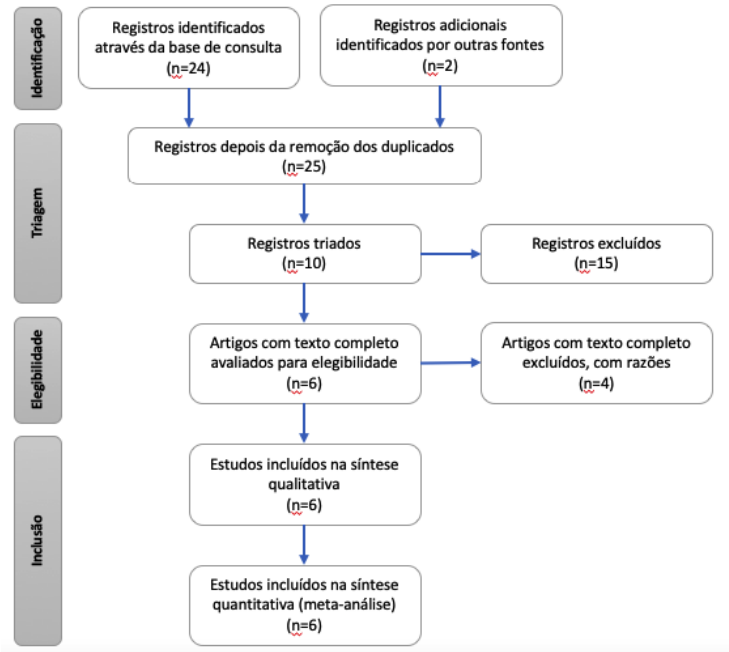
Table 1 illustrates the number of articles found with the search terms indicated in the respective column. In total, Table 124 published papers were identified that make up the corpus of this bibliometric survey, exported from SCOPUS to Microsoft Excel.

Table 1 - Localized articles and their search terms by search basis

Base	**Search terms**	**Articles**
SCOPUS	(TITLE-ABS-KEY ("agile" OR "agile method" OR "agile principle*")) AND (ALL(("cybersecurity" OR "computer security")) AND (incident AND response)	24
	Total	24

Source: prepared by the authors

Figure 11 - PRISMA-P Protocol Flowchart


Identificação
Registros identificados através da base de consulta (n=24)
Registros adicionais identificados por outras fontes (n=2)
Triagem
Registros depois da remoção dos duplicados (n=25)
Registros triados (n=10)
Registros excluídos (n=15)
Elegibilidade
Artigos com texto completo avaliados para elegibilidade (n=6)
Artigos com texto completo excluídos, com razões (n=4)
Inclusão
Estudos incluídos na síntese qualitativa (n=6)
Estudos incluídos na síntese quantitativa (meta-análise) (n=6)

Source: prepared by the authors

Figure Figure 11 the flowchart of the PRISMA-P protocol containing step by step in which, from 26 documents, after screening, the results of 10 documents were obtained. Advancing to the eligibility phase, 6 articles resulted, a number that persisted until the last phase.

Table 2 presents the results of the research after the eligibility application of the PRISMA-P protocol. Six studies included **Erro! Fonte de referência não encontrada.**in the qualitative synthesis, carried out with its reading, are shown.

4 RESULTS AND DISCUSSION

After data collection and treatment, six articles were identified, displayed in **Table 11** met the scope of the study, restricted to articles dealing with the use of agile principles in responding to safety incidents ofthe information.

Table 11 Selected resulting titles

Title	**Reference**
Rethinking security incident response: The integration of agile principles	(GRISPOS; GLISSON; STORER, 2014)
Security incident response criteria: A practitioner's perspective	(GRISPOS; GLISSON; STORER, 2015)

Title	Reference
Enhancing security incident response follow-up efforts with lightweight agile retrospectives	(GRISPOS; GLISSON; STORER, 2017)
Towards agile industrial control systems incident response	(HE; JANICKE, 2015)
Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource process agility and enterprise cybersecurity performance: A contingent resource process-based analysis	(NASEER et al., 2021)
The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework	(SMITH et al., 2021)

Source: prepared by the authors

In addition to what was mentioned in Sand ção 2, of theoretical framework, we present in the **Table 2** that summarizes the main findings of the selected publications, groupedby their authors.

Table 2 Summary of the main findings in the selected publications

Authors	Summary of findings in the literature researched
Grispos G, Glisson WB, Storer T	The authors propose in (GRISPOS; GLISSON; STORER, 2014) an agile integration into information security incident response processes with (1) iterate and incremental incident response; (2) reduction of uncertainties; and (3) continuous attention to technical excellence. The authors indicate that few studies investigate the integration of agile principles and practices within information security incident response processes. Nofurther studies for future work calling agile *incident response*. In (GRISPOS; GLISSON; STORER, 2015) proposed that organizations can benefit from an alternative approach to dealing with and managing security incidents, identified as Security Incident Response Criteria (SIRC) and that they could integrate with agile principles and practices. In (GRISPOS; GLISSON; STORER, 2017) investigate the integration of light agile retrospectives and meta-retrospectives into a security incident response process to improve feedback and/or follow-up efforts.
Y He, H Janicke	The authors examine in (HE; JANICKE, 2015) the incident response procedure of an *Industrial Control System* (ICS) from a managerial perspective, identifying the unique incident response characteristics of industrial control systems and proposes a framework to improve incident response capabilities. In particular, it evaluates the benefit of agile values to address specific incident response characteristics of industrial control systems.
Naseer et al.	The authors propose in (NASEER et al., 2021) that organizations can obtain agility in responding to security incidents: (1) allowing flexibility in incident response (2) allowing speed in incident response; and (3) enabling innovation in incident response.
R Smith et al.	The *Agile* Incident Response framework for Industrial Control Systems (AIR4ICS) was developed by the authors to integrate agile techniques in the field of Cybersecurity to respond to incidents. The *framework* provides a dynamic approach to improving situational awareness, information sharing, collective decision-making, and responsiveness within the unique ics context. AIR4ICS ensures that the relevant information is clearly and concisely available, providing resources and techniques to assign and present the information to the entire group. By ensuring that all team members have a greater understanding of the overall response strategy, they will be better able to make informed decisions in their own work. The modular design ofthe *framework* means it can be adapted to suitother work practices, skill sets and priorities of organizations. The authors point out that *the framework* improves communication, promotes the sharing of information between areas of knowledge and increases external access. Ultimately, AIR4ICS provides a dynamic decision-making framework that enables incident response teams to manage uncertainty and unpredictability to reduce the time it takes to restore normal operations.

Source: prepared by the authors

When constructing the synthesis of the articles selected in this study, we identify as research gaps the use of agile principles in responding to information security incidents in productive systems but beginning to be filled in the most recent researches such as Smith et al. (2021)the work of .

5 FINAL CONSIDERATIONS

The present work of systematic review of the literature is located in the field of information security emphasizing the response to safety incidents in production systems. A vision related to the approach to agile principlesand values, which has been used outside the area of software development, was *added*.

The objective of the research was to performa systematic review on scientific article databases to identify the works that deal with the agile approach in the processes of response to information security incidents.

In response to the research question "What results are found in the literatureon the use of the principles of information security in the production systems? ", the systematic review carried out found six articles addressing the use of agile principles in responding to information security incidents.

Thus, the research demonstrated a gap on the use of agile principles in responding to information security incidents. Although there has been several researches on the agile method and information security, when applying filters for agile principles and response to information security incidents, the small number of jobs was exemplified.

The AIR4ICS framework proved to be the closest to a practical proposal for applying agile principles in incident response.

The result contributes to filling the indicated gap demonstrating the need for further research on this theme. It is envisaged that this area could have greater contributions throughout future research. In addition, the AIR4ICS framework can be enhanced with its application and adaptation to other areas besides industrial control systems.

REFERENCES

AHMAD, A.; HADGKISS, J.; RUIGHAVER, A. B. Incident response teams - Challenges in supporting the organisational security function. **Computers and Security**, v. 31, n. 5, p. 643–652, 2012.

ALCÁCER, V.; CRUZ-MACHADO, V. **Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing SystemsEngineering Science and Technology, an International Journal**Elsevier B.V., , 1 jun. 2019.

AMORIM, A. C.; MIRA DA SILVA, M.; PEREIRA, R.; GONÇALVES, M. **Using scrum for implementing IT governance with COBIT 5**. Proceedings - 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference, EDOC 2018. **Anais**...Institute of Electrical and Electronics Engineers Inc., 14 nov. 2018.

BECK, K.; BEEDLE, M.; VAN BENNEKUM, A.; COCKBURN, A.; CUNNINGHAM, W.; FOWLER, M.; GRENNING, J.; HIGHSMITH, J.; HUNT, A.; JEFFRIES, R. **Manifesto for Agile Software Development**. Disponível em: <http://agilemanifesto.org/>. Acesso em: 22 ago. 2020.

CICHONSKI, P.; MILLAR, T.; GRANCE, T.; SCARFONE, K. NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide. **National Institute of Standards and Technology (NIST)**, 2012.

FOWLER, M.; HIGHSMITH, J. **The Agile Manifesto**. [s.l: s.n.]. Disponível em: <www.martinfowler.com/articles/newMethodology.html>.

GALEGALE, N. V.; FONTES, E. L. G.; GALEGALE, B. P. Uma contribuição para a segurança da informação: Um estudo de casos múltiplos com organizações brasileiras. **Perspectivas em Ciencia da Informacao**, v. 22, n. 3, p. 75–97, 1 jul. 2017.

GRISPOS, G.; GLISSON, W. B.; STORER, T. Rethinking Security Incident Response: The Integration of Agile Principles. 2014.

GRISPOS, G.; GLISSON, W. B.; STORER, T. Security Incident Response Criteria: A Practitioner's Perspective. **The 21st Americas Conference on Information Systems (AMCIS 2015)**, 2015.

GRISPOS, G.; GLISSON, W. B.; STORER, T. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. **Digital Investigation**, v. 22, p. 62–73, 1 set. 2017.

HE, Y.; JANICKE, H. **Towards Agile Industrial Control Systems Incident Response**. BCS Learning & Development, 2015.

LIU, X.; QIAN, C.; HATCHER, W. G.; XU, H.; LIAO, W.; YU, W. Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. **IEEE Access**, v. 7, p. 79523–79544, 2019.

MODARRESI, A.; SYMONS, J. **Technological Heterogeneity and Path Diversity in Smart Home Resilience: A Simulation Approach**. Procedia Computer Science. **Anais**...Elsevier B.V., 2020.

NASEER, A.; NASEER, H.; AHMAD, A.; MAYNARD, S. B.; MASOOD SIDDIQUI, A. Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. **International Journal of Information Management**, v. 59, 1 ago. 2021.

PAVLENKO, E. Y. Model of Cyberattacks on Digital Production Systems. **Automatic Control and Computer Sciences**, v. 53, n. 8, p. 1017–1019, 1 dez. 2019.

PFLEEGER, S. L. **IMPROVING CYBERSECURITY INCIDENT RESPONSE TEAM (CSIRT) SKILLS, DYNAMICS AND EFFECTIVENESS**. Rome, NY: [s.n.]. Disponível em: <http://www.dtic.mil>.

RIGBY, D. K.; SUTHERLAND, J.; TAKEUCHI, H. Embracing Agile. **Harvard Business Review**, v. 94, n. 5, p. 40–50, 2016.

RUEFLE, R.; DOROFEE, A.; MUNDIE, D.; HOUSEHOLDER, A. D.; MURRAY, M.; PERL, S. J. Computer Security Incident Response Team Development and Evolution. **IEEE Security & Privacy**, v. 12, n. 5, p. 16–26, 2014.

SHEDDEN, P.; AHMAD, A.; RUIGHAVER, A. B. Organisational Learning and Incident Response: Promoting Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process Effective Learning Through The Incident Response Process. 2010.

SMITH, R.; JANICKE, H.; HE, Y.; FERRA, F.; ALBAKRI, A. The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. **Computers and Security**, v. 109, 1 out. 2021.

STEFANI, C. E.; FEITOSA, M. D. Colaboração no Desenvolvimento Ágil de Software: Um Estudo a Partir da Visão dos Participantes do Processo Produtivo. 2019.

WALKER-ROBERTS, S.; HAMMOUDEH, M.; ALDABBAS, O.; AYDIN, M.; DEHGHANTANHA, A. Threats on the horizon: understanding security threats in the era of cyber-physical systems. **Journal of Supercomputing**, v. 76, n. 4, p. 2643–2664, 1 abr. 2020.