Care and Feeding of Your Security Champion

Martin Gilje Jaatun and Daniela Soares Cruzes
Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway
{martin.g.jaatun, danielac} @sintef.no

***Abstract*—In agile software development, adoption of security practices poses challenges, often because security activities are not prioritized, or because the practitioners are not able to see the relevance and importance of the activities to the improvement of the security in the project. In many teams, security activities can be seen as an innovation and as such, there is a need for a champion to realize these innovations in the teams. Security champions make software security possible. Even though all developers need to know a minimum of software security, every team needs someone to lean on when the ride gets rough – and that person is the security champion. In this paper we present the results of a case study with security champions and possible steps for establishing and maintaining this role in agile teams.**

***Index Terms*—software security, security champions; secure software engineering; build security in**

I. Introduction

Agile development methods have gained widespread adoption in the software industry, and agile methods are now used for all types of software development and for various types of systems, including very large development projects. In the opposite direction, current evidence shows that security work is often neglected in agile projects [1], [2]. Software security is about creating software that can withstand a malicious attack [3], through activities and practices that seek to minimize the introduction of security-related bugs and flaws in software systems. This implies that software security does not happen by itself, specific work practices need to handle this aspect in order to ensure that security will be addressed by the software development team [4]. In agile software development, adoption of security practices poses different challenges, often because security activities are not prioritized, or because the practitioners are not able to see the relevance and importance of the activities to the improvement of the security in the project [5].

In many agile teams, there are currently no explicit software security activities; this implies that introducing software security activities can be seen as an innovation. Following Rogers definition of innovation [6] : "Innovation is a broad category, relative to the current knowledge of the analyzed unit. Any idea, practice, or object that is perceived as new by an individual or other unit of adoption could be considered an innovation available for study". Adopting and implementing such innovations include persuasion of the team members, and also establishing and maintaining a systematic and holistic approach to security on a daily basis once that teams are deploying software continuously. Therefore, there is a need to make careful examination of which methods to introduce in order to ensure a sustainable security program in the software teams practices. The traditional focus of the software companies has been on which activities to include, without focusing on how to manage the adoption and implementation processes for these activities. We argue that there are lessons to be learned from other studies of innovation in (e.g.) information systems on how to structure the teams for facilitating the adoption of innovations.

In this paper we investigate the following research questions:

1) What is an effective way to introduce and maintain a security champion in agile software teams?
2) How are software companies applying the six Open Web Application Security Project (OWASP) action steps that enterprise leaders can take to breed security champions?
3) What can we learn from adoption of Product Innovation to improve the process or establishment and maintenance of security champions?
4) What are the challenges companies are facing during this process?

This paper is organized as follows: In Section II we present some background on the role of champions in promoting innovations in general, and in security in particular. We then present the cases in the context of which we have been studying the emergence of a security champion approach in Section III. We discuss our findings in Section IV, and conclude in Section V.

II. Background

The concept of champions is not restricted to security; in the following we will look at existing work on the need for champions for diffusion of innovations in general, before zooming in on security champions.

A. Champions of Innovation

An innovation can be any idea, product, process or object that is perceived as new to an individual or group [6]. Innovation can take many forms, and can be incremental, in which small changes occur based on current experience; radical, where a breakthrough in science or technology provides a new change; or modular, where there is a change in concept within a component of a larger system [7]. One of the necessary components of an innovation is the ability of the innovation

to improve some aspect of the adopter's performance of a work task [8].

The primary role of innovation champions in promoting innovation is embodied in the framework for innovation diffusion developed by Rogers [6] based on more than 20 years of research. Rogers defines innovation diffusion as the process by which an innovation is communicated through certain communication channels over time among the members of a social system. Rogers proposes that the innovation diffusion process takes place in five stages:

1) Knowledge is the stage where a potential adopter learns about the existence of an innovation and gains some understanding of it.
2) Persuasion is the stage where a favourable or unfavourable attitude towards an innovation is formed.
3) Decision is the stage where activities are undertaken which lead to the adoption or rejection of an innovation.
4) Implementation is the stage where an innovation is actually put to use.
5) Confirmation is the stage of reinforcement for an adoption decision which has already been taken.

Information about the existence of an innovation will be of interest to potential adopters in the early stages of the innovation-decision process, and evaluative knowledge is mainly sought in the persuasion and decision stages, e.g. the relative advantage of the innovation over, and its compatibility with, existing conditions; its ease of understanding; whether it can be easily piloted. This information is essential for reducing uncertainty about an innovation's consequences, and is most often sought from trusted peers. Rogers also indicates that interpersonal and local communications are relatively more important at the persuasion stage. Studies of product innovation success have also shown that champions are influential in overcoming barriers to adoption within organizations.

According to Weidman et al. [9], the term technology or innovation champion is used to identify leaders in the innovation process. Other terms include opinion leaders, facilitators, or change agents. In order to function effectively, a champion must have access to the required resources (including intra-organizational networking skills), as well as past experience with the innovation process [9]. Traditionally, "champion" has not been part of anybody's job description; rather, this is a role which some people in the right place of the organization have taken informally upon themselves.

According to Beckett and Berendsen [10], for an innovative idea to go all the way you need a champion who "shows persistence, belief and commitment"; this is also supported by Howell [11]. This implies that not only do you need support for the individual idea, but also to the innovation process itself.

Howell [11] studied 72 innovations in 38 companies, and discovered that there are personal characteristics and behaviors that differentiate effective champions from ineffective ones, but that it is also imperative to be able to prioritize in terms of choosing which innovations to back. Howell states that effective champions:

- convey confidence and enthusiasm about the innovation
- enlist the support and involvement of key stakeholders
- persist in the face of adversity

As Howell [11] puts it, "Relying on their personal networks inside and outside of the organization, they scout widely for new ideas and opportunities to pursue."

Howell [11] claims that effective champions exhibit the following behaviors:

- Scout widely for new ideas and information. Rely on personal networks.
- Wide general knowledge, breadth of experience, diverse interests.
- View role broadly, well informed about issues that affect the organization.
- Frame idea as an opportunity. Tie idea to positive organizational outcomes such as profitability, enhanced reputation, or strategic advantage.
- Use both formal and informal selling channels.
- Internal control: belief that events can be influenced by them.
- High self-monitors: analyze potential reactions of influence targets and tailor their selling strategies to be maximally persuasive.
- Extensive strategic and relational knowledge.

Howell [11] concludes with seven action steps that enterprise leaders can take to breed, rather than block, potential champions in their organizations:

1) Recruit and select potential champions even if they are difficult to manage.
2) Coach for skill development. Not only technical skills but also for leadership, communication and problem solving skill.
3) Mentor for career development, supporting on building network and fostering ideas.
4) Let champions volunteer for assignments that they crave.
5) Recognize innovation achievements with rewards and other recognition of achievement of results.
6) View failure as a learning opportunity and help champions learn from failure.
7) Raise the profile of champions letting them "infect others" with their passion.

B. Champions for Security

The security champion is not a new construction for software security, it has cropped up in different circumstances over the years. Boström et al. [12] advocated "adding a security expert to every team" as a solution to the software security problem, and Gary McGraw et al. [13] have been touting "the satellite" as a natural complement to the Software Security Group[1]. SAFECode[2] is a "global nonprofit organization that brings business leaders and technical experts together to exchange insights and ideas on creating, improving and

[1]In later versions of the Building Security In Maturity Model (BSIMM) report, it is formally acknowledged that "the satellite" is a synonym for "the security champions"

[2]https://safecode.org/

promoting scalable and effective software security programs". It is led by a number of high-profile security expert volunteers, most notably with Steve Lipner (former head of the Microsoft Security Development Lifecycle (SDL) team, and co-author of "The Security Development Lifecycle" [14]) as Executive Director. SAFEcode recently published a series of blog posts titled "Month of Champions", later conveniently collected as a standalone report [15], presenting good practice on building and maintaining a Security Champion program.

The SAFEcode report [15] warns against ad-hoc measures, as they (predictably) are difficult to sustain in the long run. A security champion should be an active software developer that contributes to identifying and *solving* security issues early in the software development lifecycle (SDLC). SAFEcode recommends that the Security Champion should be a full-time (or near full-time) function who will be responsible for (among other things) code review and architectural analysis efforts, contribute to security awareness, and help integrate security into the SDLC. OWASP [16] counters that 20% should be enough effort by the security champion when starting out – but this will of course vary from organization to organization. To this we could add that there is also a social aspect to the security champion role being a part-time one, as it reinforces the idea that a security champion is one that helps solve problems, not one who only creates extra work.

Engineers, developers and architects can all become Security Champions, but Product Owners and Program Managers are probably too busy to be able to dedicate enough time to the task. The latter two can however provide valuable support for the Security Champions by communicating the importance and value of the security work to the rest of the organization. Security champions must of course be conversant in the software development tools and methodologies used in the team, in addition to specific secure software development and deployment skills [15]. Additional skills include threat modeling and incident response; the latter will become increasingly important in organizations that move toward the DevOps paradigm [17]. If Security Champions are to provide the glue between security and development, they will also need the skills to be effective.

The OWASP community defines the security champion role as a key element of an AppSec team, since they create a cross-functional team focused on Application Security [18]; they are active members of a team that may help to make decisions about when to engage the Security Team; and the Security Champions act as the "voice" of security for the given product or team and; they also assist in the triage of security bugs for their team or area.

The OWASP community proposes the following activities for the Security Champion Role:

1) Actively participate in the AppSec JIRA and WIKI;
2) Collaborate with other security champions;
3) Attend weekly meetings;
4) Single point of contact for their assigned team;
5) Ensure that security is not a blocker on active development or reviews;
6) Assist in making security decisions for their team;
7) Help with QA and Testing

The OWASP security champions playbook [16] identifies six steps to building a security champion program, as illustrated in Fig. 1. More specifically, the steps entail:

Identify teams: Start with enumerating products and/or services, and then list teams per product. Product owner and team manager are then easy to identify, and the different technologies (programming languages etc.) used by each team are identified.

Define the role: Measure the software security maturity level [4] in the teams, and identify places where a security champion could make a difference. Document the defined roles in an unambiguous manner.

Nominate Champions: Introduce the idea and get buy-in on all levels. Once approval is secured, identify potential candidates with help of team leaders, and officially nominate them as part of your security meta-team.

Set up communication channels: Set up mailing lists and chats, and organize (e.g.) bi-weekly (face-to-face) sync-ups.

Build solid knowledge base: Document the tacit knowledge, provide a security meta-team page with defined roles, best practices, known risks and vulnerabilities, etc. Checklists are particularly valuable when initiating the program.

Maintain interest: Make sure to keep the champions enthusiastic and focused by organizing periodic workshops, encouraging attending security conferences, sharing recent application security news via the communication channels, and creating a physical or virtual "champions' corner" with a library and other useful resources.

III. Research Context

This research has been performed as part of the SoS-Agile research project[3], which investigated how to meaningfully integrate software security into agile software development activities. The project ran from October 2015 until March 2021. The method of choice for the project was Action Research [19] with software companies in Norway. In this project we have worked together with the companies to introduce the security champion role.

The research was performed in two companies named here Company A and Company B. Company A is a IT company that develops products in a specific sector. The company has about 100 developers and 5 security champions. Company B is a privately held company that provides business software and IT related development and consultancy, the company has more than 200 security champions (named security engineers internally).

Data in both companies were collected during the 5 years of the research project, comprising field notes, observations, interviews, and focus groups with the security champions.

[3]https://www.sintef.no/sos-agile/

Fig. 1. The Six Steps from the OWASP Security Champions PlayBook [16]

A. Company A

Company A is an agile software organization spread over three different geographical locations. There are about 15 developers working at the head office, with about 40 developers at location (2), and about 15 developers at location (3). Location (2) is a popular outsourcing destination, whereas location (3) exists due to the presence of a major customer.

In 2017, the company hired a new "software security person" (which we will refer to as the Application Security Officer or ASO) to be the driving force behind their software security program, after the previous person moved into a sales and marketing function in the company.

Company A is divided into five teams, and each team has appointed a security champion who has regular meetings with the ASO. The ASO created the description of the role based on the OWASP proposal. The recruitment in the teams has primarily been performed by identifying persons with an interest in (and previous knowledge of) security. The ASO has also established a bi-weekly 30 minute meeting with the Security Champions, a Security Guild meeting where all the Security Champions would participate and hear about news and other approaches for security in the Company.

The ASO has done a self-assessment of the software security in the company based on the Building Security In Maturity Model (BSIMM) [13] to identify which areas to improve first.

In the beginning, the security champions were working on an on-demand basis directed by the ASO. After about 6 months, the ASO performed a retrospective with the Security Champions and realized that there was a clear need to have some pre-allocated hours for the Security Champions to work on the security-related activities. The ASO then ensured that 8 hours per week were pre-approved to work on security-related activities. These hours could be used by the security champions or be delegated to team members.

The communication between the ASO and the security champions was done via meetings, emails and a slack channel with all security champions.

The skill development was performed individually depending on the needs of each security champion and also on the needs for the team. Some strategies used by the ASO in this respect were:

- One to one bi-weekly meetings where there are discussions on which topics are needed by the team and by the security officer. In some meetings it was necessary to go through some specific subject together;
- Security Guild: a meeting were all security champions meet and talk about some security subject;
- The ASO created a page with different links for learning materials that the teams could need;
- The ASO together with the Security Champions created a list of conferences and courses that can be interesting for the development of the skills of the security champions.

The program has been running for 1,5 years, and it is about having a balance between giving challenging requests to the security champions, but also requests that they are able to deliver in the expected time and quality. This is something that only happens when the security champion becomes more mature in the role. The ASO has also worked on recognizing the maturity of the security champions and have focused on spreading innovative approaches inside the teams to the other security champions through the Security Guild meetings.

B. Company B

Company B is also an agile software organization. Company B has more than 8500 employees and operates across the entire Nordic region along with Benelux, Central and Eastern Europe.

Since 2015 the company has a service for "security engineers", which is a a part time role within a Software Delivery Team. By 2020 there were more than 300 engineers with this role. As in company A, the recruitment in the teams has primarily been performed by identifying persons with an interest in (and previous knowledge of) security. In the cases in which this identification was not possible, the company has appointed engineers to this role.

On the role description the company has established the following purpose and background to the role:

- Spread and increase security awareness/culture;
- Share knowledge on the Security Program and how to use it;
- Scale security work in an efficient and tested way (recommended by SANS, OWASP etc. and used by many large organizations);
- Get the opinion from the security team about upcoming changes or questions to the Security Program;
- Participate in the Security Guild Meetings to get information about upcoming changes in the Security Program and to share information, best practice or questions among teams;
- Engage and introduce "non-security" people into security;

The Security Guild has meetings twice a month to discuss and share information, there's also a Slack channel where questions and discussions can be held. The security engineers meet the security team on demand when there is a need to discuss the security actions in the company. The security

engineers are also responsible for facilitating the filling of the security self assessment of the security in the product in which he/she is part of the team. The self-assessment is inspired by OWASP SAMM 2.0, but with more detailed questions about the security of the product.

The skill development is also performed on demand, the company uses the different security activities to provide hands-on training of security. For example on the static analysis tools, on doing threat modelling etc.

The program has been running for 5 years. The company keeps an ambidextrous approach to security [20] in which the company keeps a Top-down and bottom-up approach to security focusing on empowering the security engineers to build a self-managed approach to security inside the teams.

IV. Results

As shown in Table I, both companies has followed the OWASP [16] approach when launching their security champion program, but also implemented some steps from the Howell [11] approach.

On the first research question, our results shows that there is a need for further investigation on "how" to create and maintain the initiative of having Security Champions on the Agile Teams. The results show that if one follows the OWASP Playbook, one may miss some specific points on the "how". On the other hand, if one decides to follow the steps outlined by Howell, one may miss important steps as well, as for example the "Definition of the Role". This is an important step on the establishment of the role, but little focus is given on this by Howell. The case studies also show that it is not sufficient to only appoint the security champions, but the delegation of authority on security is needed to make the program work.

Clearly the type of Champion that Howell studied was the product innovation champion, which has very different characteristics, behavior and needs than a Security Champion as we advocate for in this paper. Hence, we can be inspired by Howell's work, but we must take this fact in consideration. For example, regarding Howell's steps 6 and 7, we had no evidence in our study regarding whether these are necessary in a software security program for agile projects, or which approaches could be effective to the security champions approach. On the other hand, it is clear that the champions need a minimum of visibility and "clout" to get their work done; in Company A much of this is ensured by the existence of the ASO, but we envision that over time this might rub off on the security champions.

The empowerment to do the job is also a step that is not emphasized enough in the OWASP approach. More emphasis is needed on giving the security champions the tools they need to make better security decisions and flexibility regarding these decisions. Both developers and security champions need to be encouraged and equipped to reach out to experts within the organization when a given situation is beyond their skills. Empowerment is also achieved by fostering trial and error mindset, but this is also something that was not evidenced in the software companies in the study.

On the diffusion of innovations perspective, our experience is that the security champions could be more aware of the stages of the innovation process as described by Rogers [6]. Specially we see that the security champions could have benefited from more persuasion techniques to improve the process of adoption of the security activities, and follow up the implementation thinking of how to learn more about the effects of the innovation to the software development process. We have argued elsewhere [21] that the security champion(s) would be the natural link between a Chief Information Security Officer (CISO) and the developers in development organisations that do not have an ASO as Company A did. On the other hand, Company A *did not* have a CISO at the time of the study, so we have no insight on how the role of the ASO in that company would change once a CISO was also present in the company hierarchy. Company B did have a CISO, but this role was not involved with the application security and software security activity.

On the challenges for implementing a security champions approach in the organizations, there are two that are most prominent: the volunteer vs. appointed security champion selection, and the competence management of the security champions. On the first, especially in large organizations is not so easy to fill in all teams with volunteers to the security champion role. When security champions are appointed, there are higher chances that the security champion will not perform the role as expected, but focus on compliance and doing the minimum required for the security activities of the team. On the competence management of the security champions, the challenge is to define which type of training should be established; it is not always effective to have traditional class-room training sessions, specially for larger organizations. Company B uses a hands-on strategy to perform training of the security champions, they provide a team of security experts to assist the security engineers (i.e., security champions) on the execution of the security activities defined in the security software development lifecycle; for example when performing threat modeling, a security expert helps to ask the right questions on the data-flow diagram.

V. Conclusion

Whereas we do not begrudge anybody having a full-time Security Champion, this would be difficult in smaller organizations. However, the Security Champion tasks should have priority, and pains should be taken to ensure that the Security Champion has some time to do security tasks every day. For smaller organizations, we believe it would be better to have (say) 5 persons with a 20% security champion role, than a single Security Champion having to spread her time between five different teams.

Management support is crucial. However, simply hiring a "security person" and expecting that person to swoop in to fix security problems is a doomed strategy. McGraw has stated that it is easier to take a developer and train her to become a software security person that to take a security person and teach her software - and clearly, if you are starting from scratch

TABLE I
COMPARING ADVICE FROM OWASP AND HOWELL WITH EXPERIENCES FROM THE CASE STUDIES.

OWASP	Howell	Observations and Comments
(1) Identify teams	——-	In both case studies, it was established that there will be one security champion per team. The teams were already defined in the organization. Other activities proposed in the OWASP Playbook for this step did not resonate with the case study.
(2) Define the role	——-	This is an important step, and the OWASP was very good on defining the initial draft for the role [16]. The role definition was established in both case studies, defining what is expected from the role. In Company A, after some time there became clear the need to have some pre-allocated hours for the Security Champions to work on the security related activities. And it was established that the Security Champions could allocate 8 hours per week to work on security related activities.
(3) Nominate Champions	(1) Recruit and select potential champions	The recruitment of the security champion in the teams has been made based on identifying team members with a personal interest and previous knowledge of security. In Company A, there was little leeway with respect to choice from software teams that are usually small. In Company B, in the cases where it was not possible to find a volunteer, the security engineer was appointed by the product manager.
(4) Set up communication channels	——-	This step is very important and not explicitly mentioned by Howell. In the case of both companies, they have established a slack channel with the security champions, besides the pre-scheduled bi-weekly meetings, communities of practice through meetups and OWASP Chapter meetings. The communication channels were established in both companies not only to have one way communication flowing, but for building relationships between security champions, for knowledge sharing and for building a network of security champions.
(5) Build solid knowledge base	(2) Coach for skill development	The Skill development needs to be done and it is taken seriously in both companies in terms of technical skills, by providing direct coaching and hands-on training of the security champions. However, there is not a focus on the development of transformational and leadership skills, or on problem solving.
——-	(3) Mentor for career development	The Security Officer in Company A, did some mentoring of the career development including the security skills but also conferences, and other courses. In company B a security career path was created, which the security personnel can follow for further development in their security career.
(6) Maintain interest	——-	It is about having also a balance between giving challenging requests to the security champions but also requests that they are able to deliver in the expected time and quality. In the companies there was not a specific task or approach for this, other than trying to maintain the interest through the security guild meetings.
——-	(4) Let champions volunteer for assignments that they crave	In both Companies, volunteering only happened when the security champion becomes more mature in the role. In both cases, most of the time the security champions would mostly act on the top-down requests to security activities.
——-	(5) Recognize innovation achievements	It is important that the innovation achievements are recognized and spread for other security champions. They are usually evidenced in the bi-weekly meetings, and spread to the others in the security guild meetings. But sharing of experiences in both cases were scarce, and the security engineers had to be asked explicitly to do so.
——-	(6) View failure as a learning opportunity and help champions learn from failure	This point was not observed in the case studies.
——-	(7) Raise the profile of champions	This point was not observed in the case studies.

it will be much easier taking someone who is already part of the team than trying to insert an unknown quantity.

Once the security champion is in place, this person will be a natural source of support for security functionality, such as how to use cryptographic libraries, authentication functions, and key management. More importantly, though, the champion will be able to contribute to increased security awareness, but for security functions and software security in general. It's one thing to be aware of OWASP Top 10, but another to fully understand the implications of them to the product.

Our conclusion is that having someone on the team [12] to ask makes a difference on the adoption of the security activities that the company chooses to pursue as part of its software security initiative. In addition we have found that following a mixed approach of the steps proposed by OWASP and by Howell is a good strategy for establishing a security champions program in the organization.

As further work, we intend to expand our study of the practical introduction and maintenance of security champions with empirical evidence from more companies.

ACKNOWLEDGMENT

This work was supported by the *Science of Security in Agile Software Development* project (SoS-Agile), funded by the Research Council of Norway (grant number 247678).

REFERENCES

[1] I. A. Tøndel, M. G. Jaatun, D. S. Cruzes, and N. B. Moe, "Risk centric activities in secure software development in public organisations," *International Journal of Secure Software Engineering (IJSSE)*, vol. 8, no. 4, pp. 1–30, 2017.

[2] H. Oueslati, M. M. Rahman, and L. ben Othmane, "Literature review of the challenges of developing secure software using the agile approach," in *2015 10th International Conference on Availability, Reliability and Security*. IEEE, 2015, pp. 540–547.

[3] G. McGraw, *Software Security: Building Security In*. Addison-Wesley, 2006.

[4] T. D. Oyetoyan, M. G. Jaatun, and D. S. Cruzes, "A lightweight measurement of software security skills, usage and training needs in agile teams," *International Journal of Secure Software Engineering*, vol. 8, no. 1, pp. 1–27, 2017.

[5] C. R. Camacho, S. Marczak, and D. S. Cruzes, "Agile team members perceptions on non-functional testing: influencing factors from an empirical study," in *2016 11th international conference on availability, reliability and security (ARES)*. IEEE, 2016, pp. 582–589.

[6] E. M. Rogers, "Diffusion of preventive innovations," *Addictive behaviors*, vol. 27, no. 6, pp. 989–993, 2002.

[7] A. M. Blayse and K. Manley, "Key influences on construction innovation," *Construction innovation*, vol. 4, no. 3, pp. 143–154, 2004.

[8] T. M. Toole, "Uncertainty and home builders' adoption of technological innovations," *Journal of construction engineering and management*, vol. 124, no. 4, pp. 323–332, 1998.

[9] J. Weidman, D. Young-Corbett, C. Fiori, T. Koebel, and E. Montague, "Prevention through design: Use of the diffusion of innovation model to predict adoption," in *International Council for Research and Innovation in Building and Construction Conference (CIB W099 Conference 2011)*, 2011.

[10] R. C. Beckett and G. Berendsen, "Learning to compete: entrepreneurial roles exploiting knowledge spillovers," in *Knowledge Spillover-based Strategic Entrepreneurship*. Routledge, 2016, pp. 204–224.

[11] J. M. Howell, "The right stuff: Identifying and developing effective champions of innovation," *Academy of Management Perspectives*, vol. 19, no. 2, pp. 108–119, 2005.

[12] G. Boström, J. Wäyrynen, M. Bodén, K. Beznosov, and P. Kruchten, "Extending XP practices to support security requirements engineering," in *Proceedings of the 2006 international workshop on Software engineering for secure systems*. ACM, 2006, pp. 11–18.

[13] G. McGraw, S. Migues, and J. West, "Building Security In Maturity Model (BSIMM 9)," 2018, https://www.bsimm.com/content/dam/bsimm/reports/bsimm9.pdf.

[14] M. Howard and S. Lipner, *The Security Development Lifecycle*. Microsoft Press, 2006.

[15] SAFEcode, "Software security takes a champion," 2019. [Online]. Available: http://safecode.org/wp-content/uploads/2019/02/Security-Champions-2019-.pdf

[16] A. Antukh, "Security champions playbook," Open Web Application Security Project, 2017. [Online]. Available: https://www.owasp.org/index.php/Security_Champions_Playbook

[17] M. G. Jaatun, D. S. Cruzes, and J. Luna, "DevOps for Better Software Security in the Cloud," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17. New York, NY, USA: ACM, 2017, pp. 69:1–69:6. [Online]. Available: http://jaatun.no/papers/2017/secdevops-author.pdf

[18] D. Cruz, "Security champions," Open Web Application Security Project, 2016. [Online]. Available: https://www.owasp.org/index.php/Security_Champions

[19] R. Davison, M. G. Martinsons, and N. Kock, "Principles of canonical action research," *Information systems journal*, vol. 14, no. 1, pp. 65–86, 2004.

[20] D. S. Cruzes and E. A. Johansen, "Building an ambidextrous software security initiative," in *Balancing Agile and Disciplined Engineering and Management Approaches for IT Services and Software Products*. IGI Global, 2021, pp. 167–188.

[21] I. A. Tøndel, M. G. Jaatun, and D. S. Cruzes, "IT security is from Mars, software security is from Venus," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 48–54, 2020.