THE ROLE OF PRODUCT MANAGERS IN SECURING SOFTWARE PRODUCTS

Lappeenranta–Lahti University of Technology LUT

Master's Programme in Software Product Management and Business, Master's Thesis

2025

Elina Koski

Examiner(s): Professor Sami Hyrynsalmi, D.Sc. (Tech.)

Post-doctoral Researcher Andrey Saltan, Ph.D.

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

LUT School of Engineering Science

Software Engineering

Elina Koski

The role of Product Managers in securing software products

Master's thesis

2025

53 pages, 2 figures, 15 tables and 1 appendix

Examiner(s): Professor Sami Hyrynsalmi and Post-doctoral Researcher Andrey Saltan

Keywords: software, information security, software security, product management, software development

Software security is becoming a pivotal concern in the management of software products. Considering the many things that can influence the security of a software product, no role alone can be responsible for it, but the Product Manager is well-placed to drive the security work.

The Product Manager perspective into security of software products is little present in existing literature. Academic research has focused on the developer perspective and industry literature is focused on commercial success. In the agile context some literature has recognised the Product Owner as a role with influence in matters of security due to their responsibility for prioritization in the Scrum framework.

This thesis looks at existing literature to establish what kind of a role the Product Manager can have in the security of software products. The literature review is supplemented by qualitative semi structured interviews of 13 product management professionals from different Finnish organizations with strong security cultures to establish if Product Managers themselves are conscious of their role and influence in matters of security of their products and what they see to be their best means of ensuring the security of their products.

The Product Managers themselves are conscious of the influence they can have on the security of their products. This thesis argues for making security more visible and tangible to remind software product management professionals of its importance to the long-term viability of software products.

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT Teknis-luonnontieteellinen

Tietotekniikka

Elina Koski

Tuotepäällikön rooli ohjelmistotuotteiden turvallisuudessa

Tietotekniikan diplomityö

2025

53 sivua, 2 kuvaa, 15 taulukkoa ja 1 liite

Tarkastaja(t): Professori Sami Hyrynsalmi ja Tutkijatohtori Andrey Saltan

Avainsanat: ohjelmistot, tietoturvallisuus, ohjelmistoturvallisuus, tuotehallinta, ohjelmistokehitys

Ohjelmistoturvallisuudesta on tulossa keskeinen huolenaihe ohjelmistotuotteiden tuotehallinnassa. Ottaen huomioon ohjelmistotuotteiden turvallisuuteen vaikuttavien asioiden määrän, yksikään rooli ei itsenäisesti ole siitä vastuussa, mutta tuotepäällikkö on hyvässä asemassa toimiakseen turvallisuustyön ajurina.

Tuotepäälliköiden näkökulma ohjelmistotuotteiden turvallisuuteen on vähän esillä akateemisessa tai ammattikirjallisuudessa. Akateeminen kirjallisuus on keskittynyt ohjelmistokehittäjien näkökulmaan, kun taas ammattikirjallisuus keskittyy tuotteiden kaupalliseen menestykseen. Tuoteomistajan rooli on tunnistettu ketterän kehityksen yhteydessä turvallisuuden kannalta tärkeäksi rooliksi johtuen tuoteomistajan priorisointivastuusta Scrumin viitekehyksessä.

Tämä työ perehtyy tuotepäällikön rooliin ohjelmistotuotteiden turvallisuudessa kirjallisuuskatsauksen ja laadullisen semistrukturoidun haastattelututkimuksen avulla. Haastatteluiden tavoitteena oli tutkia miten tuotepäälliköt itse hahmottavat oman roolinsa ja vaikutusmahdollisuutensa ohjelmistotuotteiden turvallisuuteen ja mitä he näkevät parhaina keinoinaan varmistaa tuotteidensa turvallisuus. Tutkimusta varten haastateltiin 13 tuotehallinnan ammattilaista suomalaisista organisaatioista, joissa on vahva turvallisuuskulttuuri.

Työn keskeinen argumentti on turvallisuuden tekeminen näkyväksi ja konkreettiseksi.

ABBREVIATIONS

Abbreviations

B2B	Business to Business
B2C	Business to Consumer
CISO	Chief Information Security Officer
ISPMA	International Software Product Management Association
PO	Product Owner
SDLC	Software Development Life-Cycle

Table of contents

Abstract

Abbreviations

1 Introduction 11
2 Literature review 13
2.1 Product Managers and Software Product Management 13
2.2 Security and Software Products 18
2.2.1 Points of views to security 18
2.2.2 Selling points for security 20
2.2.3 Security of Software Products 21
3 Empirical research 24
3.1 Research questions 24
3.2 Research method 24
3.2.1 Interview planning 25
3.2.2 Participant selection 26
3.2.3 Demographic information 26
3.2.4 Interview analysis 30
4 Results 32
4.1.1 Involvement in software development 32
4.1.2 Definitions of security of software products and software security 33
4.1.3 Responsibility for the security of software products 34
4.1.4 The role of Product Managers in the security of software products 35
4.1.5 Implications of Product Managers' decisions on security 36
4.1.6 Priority of security 38
4.1.7 The best means to ensure security of software products 38
4.1.8 Organizational attitudes to security 40
4.1.9 The role of cybersecurity in product development and product security 40
4.1.10 Customer attitudes to security 41
4.1.11 Additional comments 42

4.2 Discussion 44
5 Conclusions 49
References 51

Appendices

Appendix 1. Interview questions

Figures

Figure 1: ISPMA-SPM Framework v.1.3

Figure 2: The Product Triangle, adapted from Anon & González de Villaumbrosia (2017)

Tables

Table 1. Interview participants' titles

Table 2. Educational background of interview participants

Table 3. Sectors of the interview participants

Table 4. The role of Product Manager

Table 5. The main responsibilities of Product Managers

Table 6. Categories and themes identified from interview data

Table 7. Product Managers' involvement in software development

Table 8. How Product Managers define security of software products

Table 9. Responsibility for the security of software products

Table 10. Role of the Product Manager in ensuring security of the software product

Table 11. Implications of Product Managers' decision on security of the software product

Table 12. Prioritization of security in decision-making

Table 13. The best means for ensuring security of software products for Product Managers

Table 14. Customer attitudes on security of software products

Table 15. Themes in additional comments made by participants

1 Introduction

Software is everywhere, and using software products is becoming a necessity of living in a modern society. This work has been written using a software product (Microsoft Word), information presented in it has been retrieved using a software product (Chrome), the interviews were conducted using a software product (Microsoft Outlook and Teams), just to name a few. That these software products do not endanger their user or that they have been engineered to minimize vulnerabilities, that they are updated and fixed if issues occur, is usually at least an implicit expectation that the end user has. They presume that a company would handle any glaring security concerns before launching a product.

Security in the context of software is traditionally understood through the acronym CIA, short for Confidentiality, Integrity and Accessibility (Cawthra et al., 2020). These are the three main items that need to be protected for a software to be thought of as being secure. How this is done is left up to the developers of the software to evaluate and decide.

In a software organisation, there are a variety of roles that can directly or indirectly impact the security of the software the organisation produces. Responsibility for the security of a software product seems to be up in the wind though. There is literature to suggest both that many hold the belief that responsibility for security is the responsibility of someone else (eg. Assal & Chiasson, 2018) and that if asked, many claim it has been baked into the process and it is everyone's responsibility, which is just a roundabout way of saying it is no one's responsibility. Companies are often diligent about ensuring their own IT environments are carefully managed and maintained to prevent precious company data from being compromised, but does that diligence extend to the software products they develop and sell, especially in the B2C context? It should, since according to IBM (2025) the global average cost of a data breach in 2024 was 4.88 Million USD, an increase by 10% from 2023.

No single role alone can be responsible for the security of a software product, because so many things along the development lifecycle affect it. However, as a role extensively involved in the different facets of product development and management from its inception to its eventual phasing out, the Product Manager is in an excellent position to consider the big picture and to ensure security is not only considered at the right level but built into the product.

The role of the Product Manager in this context is a little researched topic, however. Most of the existing research into the topic of software security is, justifiably, focused on the role and the point of view of the software developers. In a 2021 systematic literature mapping on secure software development, Nina et al. (2021) identified 528 papers discussing dimensions of secure software development. Some recent research does address the involvement of Product Managers, however still from a developer perspective and not very extensively.

The objective of this work is to investigate how security of software products and their development appears in existing frameworks of the roles and responsibilities of the Product Manager. This work brings the Product Managers themselves to the discussion by looking into how Product Managers themselves view their role and their means to make a difference when it comes to the security of their products. Product Managers appear to have a wide range of tools at their disposal at different stages of a software product's lifecycle to affect its security.

The work is structured as follows: Chapter 2 presents a review relevant literature and outlines the theoretical framework of this thesis. Chapter 3 discusses the empirical research conducted for this thesis and chapter 4 discusses the results of the research. Chapter 5 lays out the conclusions of this thesis and topics for further research.

2 Literature review

This chapter presents the literature review around the topics of Software Product Managers, their role and responsibilities, and the theory around software security and security of software products. The first sections of this chapter focus on the role and responsibilities of Software Product Managers and the latter sections look at software security.

2.1 Product Managers and Software Product Management

The nature of software makes the industry around it different to the more traditional manufacturing industries. Kittlaus (2022) defines products as "a combination of material or intangible goods and services, which one party (called vendor) combines and evolves in support of their commercial interests, with the intention to transfer defined rights to one or more second parties (called customers)", and software products as products "whose primary component is software". Kittlaus includes in his definition also software-intensive products.

Software is intangible, so its distribution is fast, cheap, and global. Once the software product has been manufactured, the cost of its reproduction is negligible, though the initial production costs can be expensive, and customizing software to meet the needs of a specific user group is straightforward. The market for software products is usually a winner-takes-it-all market due to the network effects that govern it. When the market is not yet matured, market entry is possible with small initial costs and there are often many small operators in the market, but as the market matures and the network effects start to accumulate, the number of products on the market decreases down to just one or two market leaders, and at that point it becomes very hard for new, small products to enter the market. (Buxmann et al. 2013, 3, 5-12; Kittlaus 2022, 18-20)

Software products are either standard off-the-shelf products sold to a large market or custom software developed to meet the needs of a specific user group. Custom software is often built in-house, or the development is outsourced to a vendor. The customer can be a business or a private user. In the business-to-business (B2B) market, the selection of a software product to fulfil a need is often a more carefully considered process based on specific company conditions, criteria, and costs. The specific criteria for companies considering their options

could include items such as functionality and the reliability of the provider. For consumers choosing between options, the process looks like the B2B side, however it often also includes personal, less objective factors, such as lifestyle, peer promotion and emotions. (Buxmann et al. 2013, 5-13)

Software products most often earn revenue in one of two ways: by a one-time charge or by charging periodically. The currently predominant way is to charge periodically for the use of a software, due to the Software as a Service business model. Charging the customer periodically for the use of the software earns the product revenue over time, and growth is based on acquiring new customers while retaining existing customers. In the initial product launch phase, the periodical charge model creates a slower growth than the one-time charge, but the revenue stream is steadier over time. (Kittlaus 2022, 21)

The role of Product Manager exists at the crux of all the different dimensions that make up a software product and is responsible for a variety of activities focused on the ensuring the viability of the product over its lifecycle. Due to the range of activities, most existing frameworks and studies into the roles and responsibilities of Product Managers recognise that for many dimensions, the responsibility of the Product Manager is as an orchestrator or as a communicator. Maglyas et al. (2013) looked at what kind of roles Product Managers commonly fulfilled in their organizations and recognized four Product Manager stereotypes for comparing Product Manager responsibilities. They called these the “essential characteristics of a software product manager” and used them to define the boundaries of the role. They identified that for Product Managers, participation in the development does not mean responsibility for the implementation of the product.

Tkalich et al. (2022) looked at Product Manager responsibilities in the Agile context, identifying product-related activities and product team related activities where a Product Manager played a role in Agile organisations. Among the activities they identified, supporting the team delivery was one in which the Product Manager was an active participant. This included “ensuring that the business, design, and technology aspects were considered” (Tkalich et al. 2022).

The International Software Product Management Association (ISPMA) has laid out a comprehensive, evolving framework for the activities and responsibilities of Product Managers, which has divided their various subject areas into core responsibilities of the

Product Manager and orchestration responsibilities, for which the implementation responsibility rests on other roles. This framework is shown in Figure 1.

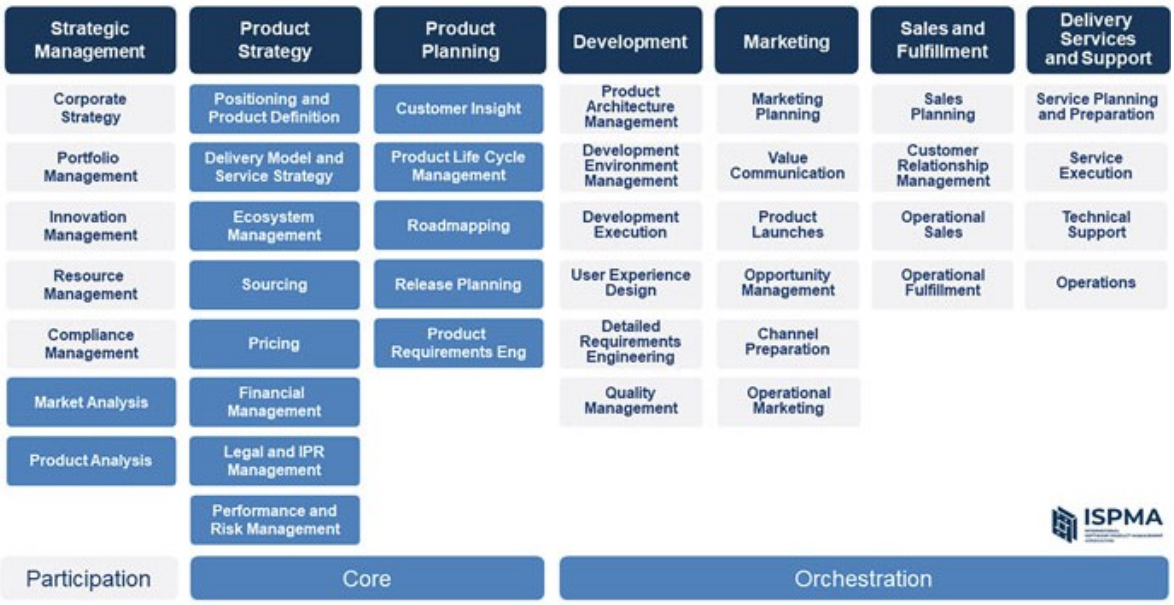

Figure 1. ISPMA-SPM Framework v.2.0 (Kittlaus 2022)

The ISPMA framework includes risk management as one of the core responsibilities of the Product Manager. Kittlaus (2022, 129) defines risk management as "continuous tracking and analysis of risks identified in connection with the software product be it in development, sales, customer use or anything else", and defines three categories of risk in conjunction with their definition of risk management: product risks, customer risks and market risks. (Kittlaus 2022, 132)

There is an argument to be made that the category of product risks and the management of those would also cover managing risks related to the security of the product, but this is not made explicit, and it is unclear if this is generally understood to be so. What Kittlaus includes in the categories as examples are risks related to things like the unique value proposition (product risk), the customer segments (customer risk), business measures (business risk), key resources (product risk), and pricing (product risk). When it comes to software, security is often understood in terms of security features or is included in the quality requirements. As seen in Figure 1, responsibility for Quality Management is not included in the Product Manager core responsibilities or their direct responsibilities.

In addition to the role of Product Manager, the Scrum framework brings in the role of Product Owner. The distinction between these two is sometimes nebulous and organization-

dependent, with some organizations employing both roles and some choosing to employ only either a Product Manager or a Product Owner. Due to this muddling of waters, this work has included Product Owners under the umbrella of product management professionals, even though strictly by the Scrum Guide (Schwaber & Sutherland 2020) their role is narrower than that of Product Managers.

While the ISPMA framework on Product Management offers a comprehensive guideline, the field of Product Management is a dynamic one, with many industry-generated insights into the role and responsibilities of Product Managers.

It is also worth looking at trade publications and resources on the matter. A well-known operator in the field, the Product School is a company offering training and certifications in product management for a fee. They also provide free online resources and have gained a steady standing in the industry. In their publication “The Product Book”, Anon and González de Villaumbrosia (2017) compare the role of the Product Manager to that of an orchestra conductor, who does not make a sound, but manages the ensemble of instruments towards a shared goal. They visualize the Product Manager responsibilities as a triangle (Figure 2), with much less emphasis on the financial aspects of product management than in the ISPMA-SPM framework. The Product School approach to product management is more focused around the phases of the product-development life cycle and whether the Product Manager has an ownership or contribution role to a phase.

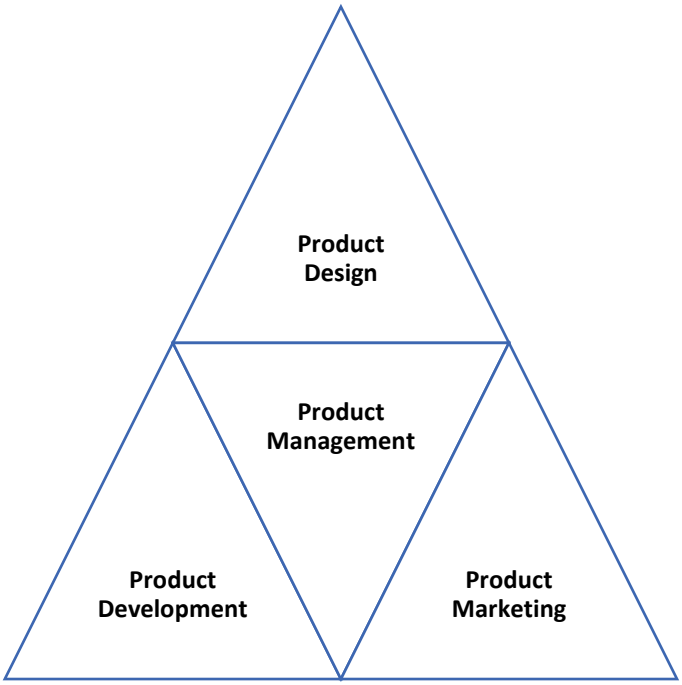

Figure 2. The Product Triangle, adapted from Anon & González de Villaumbrosia (2017)

In addition to the larger entities offering somewhat more rigorous guidance on product management, the industry has generated insights into product management, the role of Product Manager and their responsibilities in whitepapers, guides, websites, articles in industrial publications and other such freely available materials. Books on product management tend to focus on the business aspects of product management or on the development of commercially successful products (eg. Apunen 2020).

Looking at trade publications in Finland, the Finnish software company Futurice published a guide of their own to product management in 2023. This guide is focused on creation of successful products, value-creation, and organization-wide changes to enable successful product management. The document is written at a higher level, whereas security of the product can be considered a more specialized concern. The guide considers product management largely in similar terms to the ISPM and the Product School, seeing improvements in product management as a meaningful way to reduce costs, gain competitiveness, and manage resource use. Diverging slightly from the high-level overview, the guide briefly mentions environmental sustainability as one advantage to product management but makes no mention of the security of the product.

Out of all these operators, the ISPMA framework is the most comprehensive guideline into the role and various responsibilities of the Product Manager. Out of all the sources referenced

here, it is also the only one to even consider the topic of risk management, even if the concept of security does not explicitly appear in it. Notably, security is not mentioned as an explicit responsibility for any of the fields mentioned in the framework, which is concerning. Approaching the issue of effective security from the point of view of agile software development, Tøndel et al. (2019) point out that appropriate security is usually a happy accident, due to an individual with the right mindset.

2.2 Security and Software Products

Software security, cybersecurity, information security, IT security… What do we talk about when we talk about security in the context of software products? This chapter considers the terminology and concepts as well as discusses the existing research into the topic. The chapter also lays out the arguments for why organizations and Product Managers should concern themselves with the security of their products.

2.2.1 Points of views to security

We can consider the security of software products in terms of not endangering the user. This manifests not just in minimizing software flaws and fixing vulnerabilities, but also considers the hybrid threats where software, be it secure on insecure, is a component. Nominally secure software can be used to endanger its user or other users, if the software is used in ways, it was not designed for or if the software allows insecure usage of the software. The security of the software product could also be seen as more than just a sum of all the parts that make up a secure software.

From the point of view of software security, McGraw (2004) defines it as “the idea of engineering software so that it continues to function correctly under malicious attack”. Assal and Chiasson (2018) define the concept in similar terms, calling it “resistance of applications to malicious attacks resulting from the exploitation of vulnerabilities”.

The information security definition of security approaches the issue through the so-called CIA-model: Confidentiality, Integrity, and Availability. These three elements must be

present in a secure system, and ensuring these leads to high confidence that software is secure. (Ransome & Misra 2018, 2)

Much of the existing research into the topic of software security and ensuring it focuses on the role of the software developers (Weir et al. 2021a), perhaps justifiably. At first glance, pinning responsibility for software security on the developers seems logical, after all the developers are the ones in charge of writing the source code for the software. Previous research has focused on, among other things, reducing developer errors and the reasons why developers make errors (Xie et al. 2011), and developer attitudes to prescribed security (Venson 2020). Van der Linden et al. (2020) looked at the rationale developers have for the security decisions they make and found that while developers often make good decisions from the point of view of security, their reason for taking the decision is rarely security related. Guidelines and standards for secure software development exist, often created by national cybersecurity authorities (eg. Traficom 2018).

Security is often seen as an expert role requiring specific training to understand things at an appropriate level. Weir et al. (2021a) however note that software developers did not need to be security professionals to be able to conduct a viable risk assessment on their software in a workshop setting.

In the context of software development, the activity of writing source code is often the only thing that developers see as security relevant. Developers also often rely on other parties or processes for security, or they fail to recognise the relevance of security in their specific development context (Xie et al. 2011). Assal and Chiasson (2018) noted that application of security practices differs from best practices in literature, and that the company culture, hierarchy and available resources play a large part in determining if and when security practices are adopted.

The connection between security and development is often severed, which manifests in several ways, as Tøndel et al. (2020a) note. They point out that “software security is essential for information security” (Tøndel et al. 2020a, 1) but that responsibility for software security is unclear.

2.2.2 Selling points for security

Paying attention to the security of the product becomes more important as time goes by, as software products become an integral part of the society. Even the simplest software product could compromise the end user's device, their personal data, their location, or harness their device to be used in a botnet to launch Denial of Service (DDoS) attacks on infrastructure or websites.

Ransome and Misra (2018, 8) state that when it comes to sensitive information, software security is not subjective. The information is "either exposed or it is not". The same applies to your device: it is either in your control or it is not.

The perceived value of security, however, is subjective, according to Goode et al. (2015). In corporate settings, for example, security features might be seen as obstacles for work (Albrechtsen 2007), and employees might even try to circumvent them to be able to effectively do their jobs. (Caputo et al. 2016)

The main reason why companies should pay attention to the security of their product is the same as with anything: it is good business. Data breaches are expensive, there can be extensive reputational damage, not to mention legal consequences. The IBM Cost of a Data Breach Report for 2023 puts the average total cost of a data breach to be 4.45 million USD, up 2.3% from 2022 and 15.3% from 2020. (IBM 2023) Taking a Secure by Default -approach to software security can help bring down lifetime costs of a software by addressing issues when fixing them is cheapest. (Olama & Nutaro 2013)

Software products are being used by all kinds of end users with varying degrees of technical understanding and expectations with respect to the security of the products they use. Looking at a group of smart home adopters, Haney et al. (2021) found that a significant portion of their research participants placed some or all responsibility for privacy on manufacturers and some or all responsibility for security also on the manufacturers. Looking at user expectations of IoT device users, Kustosch et al. (2023) found that users expect manufacturers to respond to security vulnerabilities by patching the vulnerabilities and see this as both an appropriate and likely response. However, there exists a privacy-paradox, whereby users express a concern for privacy while doing very little to protect it in their online behaviour. Looking at this paradox, Barth et al. (2017) determined that even though

users may be aware of risks, they either determine the benefits to outweigh risks, or make biased risk-benefit calculations in favour of the perceived benefits. On the other hand, Emami-Naeini et al. (2019) found security and privacy concerns to be among the reasons why some chose not to purchase particular IoT devices. While IoT devices are not strictly software products, they are software-intensive, and as such fall under the Kittlaus (2022) definition of software products. The concepts of Confidentiality, Integrity and Availability apply to them as well.

2.2.3 Security of Software Products

Responsibilities designated by frameworks notwithstanding, are there any other pressing reasons why Product Managers specifically should concern themselves with the security of their products?

In the Product Book, Anon and González de Villaumbrosia (2017) note that Product Managers are a representative of the customer. The reason why customers buy and use products is that the product addresses a specific need that the customer has. Security of the product is mostly an implicit requirement for the customer – they want a product that fulfils their needs without endangering them as the users of the product. Some users of consumer software products rarely consider the security of the product in their purchases, or they make biased risk-benefit calculations in favour of indulging in using a popular product or service (Barth et al. 2017). As mentioned previously, Goode et al. (2015) noted that the value of security is subjective.

From the point of view of the Product Manager concerned with the commercial viability of their product in addition to requirements and the orchestration of all the supporting activities that go into the production of a product, security of their product should be an important consideration. Weir et al (2021a) talk of the need to frame security in terms of its business value and Banham (2017) points out that cyber incidents are a source of both financial and reputational damages. Citing the EY 19th Global Information Security Survey, Banham also notes that out of those respondents who had experienced a cyber incident, 49% did not know the extent of the financial damages it caused. The Economist (2017) frames the business aspect in different terms, pointing out that vulnerabilities are good business for those that wish to exploit them.

Venson et al. (2019) looked at the impacts of security on software development costs, finding that few cost-estimation models account for the impact of security on the development effort, despite the evident increasing need to adopt robust security practices. Heitzenrater and Simpson (2016) also argue for economics around the issue of secure software development, to give industry the language to make decisions and to understand when and what kind of trade-offs related to security have been made.

Jones (2015) discusses the effect of defects and their removal on the economics of software engineering, and how much software engineering effort is wasted on defect repairs and on projects that are stopped. Tøndel et al. (2019) also recognise the challenge of finding the right level of security and propose the concept of a Security Intention Recap Meeting to balance between cost, schedule and security in an agile software project. Their concept would include key stakeholders in an agile software project, including the PO, whom they mention as "a common hindrance for sufficiently prioritizing security and quality." (Tøndel et al. 2019)

Weir et al. (2022) looked at engaging Product Managers on security issues using workshops. Their approach to the issue was somewhat developer-centric, considering the initiative for the engagement to be from the developer side. The aim of the engagement was to align software security with business, and for the Product Managers to understand the relevant risks. The security-relevance of Product Managers here was seen mainly through their prioritizations.

Türpe et al. (2017) explicitly state that the role of PO is important to the success of security work in Scrum, as the person setting the work for the developers and the acceptance criteria for completed work. Türpe et al. make a distinction between product management and the role of the PO, setting product management as a stakeholder of the development team and the PO and a source for security requirements.

Just as consumers are guilty of sometimes overlooking security concerns in software products based on a biased cost-benefit analysis, the organizations responsible for creating those software products are equally guilty of assuming too much, especially if their software development is outsourced. According to Tøndel et al. (2020a), organizations expect contractors to manage software security from identification of security requirements to understanding the security risks, without appropriate checks to verify security matters are

handled. On the other hand, the same authors note in a separate publication, that the perception of what level of security is enough varies depending on the role, and that there exists a reverse bias in many organizations that without proof to the contrary, the level of security is too low. (Tøndel et al. 2020b)

For Product Managers of software products, there is a plethora of decisions they are responsible for that have either direct or indirect implications for the security of their product. For the most part, Product Managers allocate resources and make decisions about backlog priorities. If fixing of issues with the software takes backseat over developing new features, over time this will lead to technical debt that is expensive to fix and deprecates the software. Conversely, fixing accumulated technical debt takes resources from building new functionality that might make the product more user friendly, answer a growing user need or otherwise make the product more sustainable. (Olama & Nutaro. 2013; Rindell et al. 2019)

With these dimensions in mind, it could be said that the security of software products is comprised of not just the sum of all the parts of software security but also of the bigger picture.

3 Empirical research

The empirical research for this work consisted of 13 interviews. The goal of the interviews was to establish a baseline of how more or less experienced product professionals see their role in the security of a software product. This chapter discusses the research questions, and the construction of the interviews. The next chapter discusses the results from the interviews.

3.1 Research questions

This thesis has three research questions it seeks to answer. The first question is: *What is the role of the Product Manager in ensuring the security of software products?* The goal of this question is to establish what role, if any, the Product Managers have in security of software products.

The second question is: *How do Product Managers see their role in the security of software products?* This question was intended for establishing a baseline of how Product Managers themselves see their role and its relationship with the security of their software products.

The third question is: *What are the best tools a Product Manager has for ensuring the security of their software products?* With this question the aim was to see what kind of things Product Managers themselves identify as having at their disposal that are effective for impacting security and at what stage of the development lifecycle these means would be utilized.

3.2 Research method

The research method for this thesis was grounded theory based on interviews. The aim of this work was to explore a hypothesis based on professional experience without necessarily reaching a definitive answer (Bakker, 2019). Based on the literature review, semi structured qualitative interviews using qualitative content analysis for the analysis of the interviews were conducted to explore and confirm the initial finding from the literature review. There is little existing literature on the topic of security of software products from the point of view

of Product Managers, and the aim of the research was to gain insight into how Product Managers see their own role, therefore qualitative interviews were chosen as the means to explore the issue. (Kallinen et al. 2021)

There were 13 interviews conducted, with individuals either currently working in product management or with an extensive background in product management. All interviewees were from organizations with a strong security requirement for their products.

Interviews were conducted in Finnish and all participants were Finnish. Interview questions were in both English and Finnish and participants were shown both forms to mitigate the risk of differences in handling translated terminology. All interviews were conducted using Microsoft Teams, recorded, and transcribed for analysis.

3.2.1 Interview planning

The aim of the interviews was to research how the participants see their role as Product Managers as it relates to the security of their products. To make interview participation easier on the participant, it was decided that interviews would be conducted via Microsoft Teams. This also enabled recording of the interview and storage of the recording on university Teams.

The interviews were planned so that they would not take up more than an hour of participant's time. The interviews were also planned so that the one hour time limit would not be exceeded even if the participant wanted to elaborate at length on a point.

The questions were shown to participants in both English and Finnish to minimize misunderstandings of terminology. To begin with, the participant was introduced to the background of the research.

The first section of the interview elicited background information on the participant, their organization and the types of products they work with. The second section contained questions to elicit the participant's views about being a Product Manager and their main responsibilities. In the case of expert interviews, the questions sought to find their views about how these should be arranged.

The third section combined Product Management with security issues and the participants were asked to consider terminology, responsibilities, and roles when it comes to security. The aim was to see how the participants define the key concepts of software security and security of software products and to see how they consider the responsibilities and roles regarding security. Based on previous research into software developers' attitudes to security (Van der Linden, 2020; Xie et al. 2011), where responsibility for security was very strongly seen as somebody else's responsibility, be it a designated security unit or a specialist, the aim was to see if this carried over to Product Managers. This section also sought to elicit from the participants what they considered to be best means of ensuring security in software products.

The fourth section elicited some more information on the organizational attitudes to security in general and towards their products. The section asked about existence of a separate cybersecurity unit and its role. This question was included especially to see if there was a correlation between answers to this question and answers to the question regarding responsibility for security. Finally, the participants were asked for any additional remarks they might have thought of during the interview.

3.2.2 Participant selection

Because the topic of the interviews concerned security and to allay concerns of phishing attacks or scams, most of the interviews were elicited from the author's network. To increase the participant pool, elicitation was snowballed out to current colleagues of author's past colleagues and to colleagues of network contacts.

In eliciting participants, emphasis was put on participants having product management experience and not on any information security experience. Apart from one, the participants did not have significant information or software security experience.

3.2.3 Demographic information

The interview duration varied from 17 minutes (shortest) to 46 minutes (longest). Most of the interviews lasted for around 25 minutes. The shortest interview was conducted with a current colleague of the author.

All interview participants were either currently working in or had past working experience from product management in a software context. Out of the participants, six had the title of Product Manager, two were Product Owners and five were either experts in the field or previously worked as Product Managers. Table 1 outlines the participants and their titles. The amount of work experience in product management varied from less than a year to more than 20 years. All participants had been in the workforce for more than three years, with some of the participants having more than 30 years of general working experience. The participants were not asked to specify how long they had been in work life.

Table 1. Interview participants' titles

Title	Responses
Product Manager	Participant 1, Participant 4, Participant 5, Participant 6, Participant 8, Participant 11
Product Owner	Participant 7, Participant 13
Expert interviewee	Participant 2, Participant 3, Participant 9, Participant 10, Participant 12

Apart from one participant, the interviewees were male. Also apart from one, the participants had at least a bachelor's level degree from a university or a university of applied sciences (UAS) in Finland, though not necessarily in an IT related field. Even though the sample size is small, the number of participants with Bachelor of Business Administration (BBA) degrees is noteworthy. Most Finnish UASs offer BBA degrees programmes in Business Information Technology, but the participants with a BBA did not specify if their degree was from such a degree programme. Table 2 shows a breakdown of the educational backgrounds of the interview participants. Where only one participant answered with a particular degree, the answers have been grouped into "Other degree".

Table 2. Educational background of interview participants

Degree	No. of responses
Bachelor of Business Administration (BBA)	5
Bachelor of Engineering (BEng)	2
Master of Science in Technology	2
Other degree	4

Most participants were from organizations that place an emphasis on the security of their software products, with three expert interview participants not working currently with any products. The participants were from organizations in the fields of banking, telecommunications, IT, energy production and product management consultancy. Table 3 presents a more detailed breakdown of the participants' sectors.

Table 3. Sectors of the interview participants

Sector	No. of responses
Telecommunications	5
IT	3
Banking	2
Energy	1
Consultancy	2

The organizations operated both in B2B and B2C markets. The customer base for the products the participants work with range from consumers to company internal use to fire and rescue organizations.

During the interview, as part of their background information, the participants were asked to describe the role of the Product Manager in their organizations. The Product Manager role in the organization varied from a highly generalised role to a more limited one, with most of the responses mentioning the role to be a generalist role. Table 4 shows how the participants saw the role of the Product Manager.

Table 4. The role of Product Manager

Descriptor	No. responses
Generalist role / wide range of responsibilities	5
Specialist role / responsibilities are limited	2
Varies depending on organization or product	3
Product Owner role exists in addition to Product Manager	2

In one of the organisations, which more than one participant was from, the role was only recently taking shape in the organisation, with specific responsibilities still being slightly in the air. Only one of the participants specifically mentioned that the role should include responsibility for technical decisions.

The participants were also asked about their responsibilities as Product Managers. Many of the participants mentioned responsibility for the whole as a general responsibility, but then also detailed some specific responsibilities. Table 5 lists the ten most common responses from the participants.

Table 5. The main responsibilities of Product Managers

Responsibility	No. responses
Understand the customer's problems and needs / requirements	4
Answer customer needs	4
Commercial viability	4
Roadmapping	4
Responsibility for the whole	3
Communication with stakeholders	3

There were also individual mentions of, among others, making technology choices, backlog management and ensuring compliance, understanding regulation, and supporting sales.

3.2.4 Interview analysis

The answers to the questions were analysed using qualitative content analysis (Elo et al. 2014). The answers were divided into five main categories, under which the answers were then coded based on identified themes from the answers. Table 6 describes the categories and the identified themes in each category. The answers were not analysed for sentiment or relationships.

Table 6. Categories and themes identified from interview data

Category	Theme
Background information	
	Current work
	Education
	General work experience
	Work in Product Management
Organization	
	Customer attitudes to software security
	Existence of Cybersecurity unit
	Organizational attitude to security of software products
	Product Manager role in the organization
	Products
Product Management	
	Development decisions
	Involvement in software development
	Main responsibilities
	Used frameworks
Software Product Security	
	Best means of ensuring security
	Definitions
	Implications of decisions to security
	Prioritization of security in decision making
	Responsibility for security

	Role of Product Manager in security
	Secure by Default
Additional remarks	

In the analysis of the interviews, the answers were placed into five categories: background information, organization, Product Management, Software Product Security and Additional remarks. There were altogether 20 themes under these categories.

4 Results

4.1.1 Involvement in software development

The participants were asked how much they were involved in software development and what kind of decisions they made if they were involved in software development. The participants reported having a varied level of involvement in software development. Not all the participants were working strictly with software products, but more generally in the field of IT.

Table 7. Product Managers' involvement in software development

Descriptor	No. responses
Is involved in software development	8
Would like to be more involved in software development	1
Organization uses commercial off-the-shelf software, no own development	2

For one of the participants, their role and the level of their involvement in software development was still being defined. The most common tasks the Product Managers were involved in was backlog management, prioritization of features for development, and acceptance of development packages. Some reported having a say in matters related to user interface design and testing. None of the answers reported being involved in writing source code. Two of the responses specifically mention that it is necessary for a Product Manager to have some involvement in software development and one of the participants saw too much involvement in development activities being a risk in terms of neglecting the other important elements of Product Management.

"So if you're too much involved in the development then you don't have time for those important things for Product Managers, like this is in my opinion more the risk if you get too much involved in development." (Participant 12)

4.1.2 Definitions of security of software products and software security

The participants were asked to define in their own words the terms “software security” and “security of software products”. This question was included to see how the participants approached the issue and what kind of differences in definitions existed among the participants.

When asked to describe the concepts of software security and security of software products, the answers varied depending on the approach of the Product Manager to the matter. Only one of the participants had information security expertise, and such expertise was not required from any of the participants, so seeing how they approached the issue was interesting.

Security of software products was viewed by some participants from a more developer-oriented point of view, through things like good coding practices, good components, proper sanitization, integrations and API security. Some participants saw security of software products from the point of view of the use of the product being safe to its end user. Table 8 below details the different ways participants defined security of software products.

Table 8. How Product Managers define security of software products

Definition	No. responses
Good coding practices	2
Components	2
Use is safe to end user	1
Information is safeguarded	3
User feels the product to be safe	3

Software security was more straightforwardly seen as something comprised of technical decisions, access management, encryption, standards and regulations compliance, and other established security measures.

While the participants were not information security specialist, the traditional concepts of Confidentiality, Integrity and Availability were explicitly stated in three answers and in some way present in four other answers.

“So security is a whole. There’re people. There’s technology. There’re processes.” (Participant 3)

4.1.3 Responsibility for the security of software products

The participants were also asked whose responsibility the security of the software product is. This question was included to see if Product Managers perceived the responsibility to include them, or if there was indication that results from existing research on developers could apply to Product Managers as well, ie. that security was perceived as a specialist role or someone else’s responsibility.

All in all, there were three main directions the participants looked at in the question for responsibility: the Product Manager, shared responsibility, and the company management. Where the responsibility was thought to be shared, the participants did acknowledge one of the key roles to be the Product Manager, but they would not assign all responsibility to them.

Where the Product Manager was assigned responsibility, the participants mostly pointed out that this was a responsibility for the orchestration and ensuring of security, but that the Product Manager was not directly responsible for implementation. Table 9 illustrates how the participants assign responsibility for the security of software products.

Table 9. Responsibility for the security of software products

Responsible	No. responses
Shared responsibility	8
Product Manager is responsible	4
CEO / management is responsible	1

“If something bigger happens, it does enter the field of responsibility of the highest management. And they should then with their own actions and goal setting and strategy setting and budget definition enable the ability to implement secure software.” (Participant 10)

“I suppose there is some kind of a responsibility for the whole, like if my product is insecure then I’m responsible of it, I guess it would hit me, I can’t really hide in a way, but then it

means that I've failed at recognizing those situations, and I haven't asked the experts or I have knowingly or unknowingly used building blocks that are not suitable." (Participant 12)

4.1.4 The role of Product Managers in the security of software products

The participants were asked a follow-up question specifically about what the role of the Product Manager to the security of software products was. All participants recognized that the Product Manager plays a role in securing software products, however their views differed somewhat in what exactly that role entailed.

Some participants did not specify further about what kind of a role the Product Manager has but felt strongly that it existed. The experts interviewed also saw how some Product Managers could think that they would not have a role if the organization employed for example a security architect or had other such roles. The participants also often noted that they did not expect the Product Manager to be the best expert on security topics, but that they expected the Product Manager to make sure that they had the team working on the product had enough expertise to handle security topics. Individual participants also brought up very detailed security-related tasks such as threat assessments as something that the Product Manager role includes.

The answers also indicated that the participants understood well how the Product Manager could also have adverse effects on the security of their product by for example not allowing time for repairs, which shows that the participants at least understood the interdependencies that exist within product management and development.

Table 10 shows what the participants answers indicated about what kind of a role the Product Manager could have.

Table 10. Role of the Product Manager in ensuring security of the software product

Role	No. of responses
PM plays a role, no specifications	1
Allocation of appropriate resources (time, budget etc.)	4
Understanding security requirements and regulation	4
Responsibility for the whole	3
Responsible for compliance	3
Facilitate cooperation on security matters	2
Planning security matters	1
Security testing	1
Threat assessment	1
Observer role	1

“And everyone knows that bugs always exist, so you kinda have to try to react, so the Product Manager, when they often prioritize what should be done to the product next, controls to some extent the backlog, prioritizes, then it is possible for them to play it so that there is never any time to fix something or to do something with good quality or to improve the quality of some security feature.” (Participant 10)

“Absolutely they have a role in it because the Product Manager has to define, know and define the guidelines for activities, understand the use cases and the environment.” (Participant 4)

“And that much they need to know, that they see that things are not going as they should, I need to have a conversation about this.” (Participant 11)

4.1.5 Implications of Product Managers’ decisions on security

The participants were asked about which of their decisions they saw as having implications to the security of their product and why. This question was included to see how well the participants saw the wider implications of the decisions they took, or if only coding was seen to be security relevant, as was the case for developers (Van der Linden, 2020).

All 13 participants acknowledged that the decisions Product Managers make have implications to the security of their software products. These implications ranged from prioritization decisions leading to security issues to decisions about 3rd party software components carrying security threats. One participant mentioned that for them, most of the security relevant decisions are made by others, but that there was rarely anything to add to or to criticize about these decisions. Table 11 shows all the implications that the participants saw for the decisions of Product Managers.

Table 11. Implications of Product Managers' decision on security of the software product

Implications	No. of responses
All or most decisions have implications to security	5
Prioritization decisions leading to security issues and technical debt	4
Decisions related to third party software components	2
Getting the requirements right	2
Strategic product decisions (technology, target customer base etc.)	2
Choices between security and usability	1
Decisions told to vendor	1
Not demanding standards or regulatory compliance	1
Offering product for unanticipated uses	1
Security relevant decisions are mostly made by someone else	1

"Every slightly bigger decision can impact security either to improve it or to decrease it." (Participant 2)

"If you've decided to include some third-party solutions in it, and you don't really know anything about them, but include them anyways." (Participant 1)

"If you just prioritize building a lot of new things but never improve anything old or never try to decrease the technical debt or maintain the product, like this is such a classic, that this kind of decision you can then impact security a lot." (Participant 10)

4.1.6 Priority of security

The participants were asked to reflect on the types of situations where they would prioritise security. In the answers to this question, the difference in the organisational attitudes to security was rather clear, with those participants with exacting security requirements stating security to always be their main priority. For the participants working for organisations with existing but less strict security requirements, there was more room to manoeuvre in terms of priority. None of the participants considered security to not be a priority at all, however. Table 12 shows the range of answers and justifications that the participants gave.

Table 12. Prioritization of security in decision-making

Prioritization in decisions	No. of responses
Security is first priority	7
Security is important but not always first priority / context dependent	3
Prioritization is a business decision	2
Prioritization based on a risk assessment	1
Finding the right level of security is prioritized	2

“You could say that security first, it’s the first question that we consider. Is this secure? Can we implement this securely, like in our line of business that is the starting point and then we can think of other aspects.” (Participant 4)

“So like you must have some level, but isn’t it more to do with the application or product, where the, how big of a risk some information security offence is.” (Participant 12)

“Too much security starts to get really expensive.” (Participant 3)

4.1.7 The best means to ensure security of software products

Here the participants were asked to discuss what they saw as the best means for ensuring the security of their product and why. The Product Managers had a wide variety of means to ensure the security of their products at their disposal, most participants listed more than one item.

Third-party audits, penetration testing and testing in general stood out as the most popular answers. In addition to these, many participants approached the issue from a more human-centred perspective by focusing on the team and cooperation with experts on the issue. Table 13 lists all the themes identified from the participants answers and if the item is considered to be a post-development way of ensuring security.

Table 13. The best means for ensuring security of software products for Product Managers

Theme	No. of responses	Post-development	Stage of SDLC
Third-party audits and penetration testing	5	Yes	Testing, Deployment
Testing	4	Yes	Testing
Co-operation with security specialists	3	-	All stages
Trust the team	3	-	All stages
Tools and automatic scanners	3	No	Building
Product Manager's own knowledge	3	-	All stages
Motivate people to work towards security	2	No	All stages
Contractual obligations for vendors	1	(Yes)	All stages
Ensure team includes sufficient expertise	1	-	All stages
Include security in minimum requirements	1	No	Planning, Defining
Increase risk awareness	1	No	All stages
Internal security viewing	1	(Yes)	Testing, Deployment
Know the operating environment	1	No	All stages
Management commitment	1	No	Planning, Design, Deployment, Maintenance
Verification of software (eg. reverse engineering)	1	Yes	Deployment, Maintenance

“The best means is to make sure that the audit is carried out by an outside security auditor. I’m not talking about self-auditing but real outsider audits.” (Participant 6)

“Security gained from tools should by now be everywhere, it can’t be a question of costs, like all kinds of code scanners during development and vulnerability observers that work all the time.” (Participant 12)

“The best means is to get people to work in a way that the minimum requirements for security are met. To work on it that security is, here as well the 20-80 is a good way, technology is 20% and people are 80%.” (Participant 3)

4.1.8 Organizational attitudes to security

To find out more about the organisational context, the participants were asked about how their organisation handles software security and how it ensures the security of their products.

None of the participants indicated that security would be something to ignore in their organisation. Only one of the participants indicated that they would have some room to manoeuvre when it came to security matters, because they work with a product with less stringent security requirements. However, the participant also indicated elsewhere in the interview that for the products that must comply with regulatory requirements, the company takes those very seriously. For three of the participants, regulation enforced the organisational attitudes to security.

“In every place however this issue of security of software products has been handled with seriousness and it has been paid attention to. And specifically, they’ve then sought to ensure the security of those products so, that they take multiple different kinds of measures whereby they ensure that product security.” (Participant 10)

4.1.9 The role of cybersecurity in product development and product security

The participants were also asked if they had a designated cybersecurity unit in their organisation and what its role is like. This question was included to find out if the Product Managers were getting support or expecting support from a dedicated unit focused on cybersecurity.

Out of all the 13 participants, only one answered that their organisation did not have a dedicated cybersecurity unit, though this participant did mention that they do have persons filling specific information security roles, such as information security architect and CISO.

The role of the cybersecurity unit varied. For some organisations it was very much focused on the security of the organisation IT environment, creating policies and possibly consulting in audits. Some participants mentioned that they could expect their cyber security unit to provide guidance on security practices. Only one participant indicated that their cyber security unit sets security requirements for software products. One participant also answered that their information security unit produces materials for public procurement processes that the organisation is involved in.

"And you always get support from them if necessary, they have a lot of the kind of information that you might need in some individual activity and the Product Manager can pretty much rely on it, that when you ask something form them, they answer." (Participant 8)

4.1.10 Customer attitudes to security

Finally, the participants were asked to evaluate their customers' attitudes towards software security at large and more specifically towards the software produced by the participant's organisation. Table 14 describes how the participants saw the customer attitudes towards the security of their products and software products in general.

Not all participants offered an opinion on the attitudes of their customers on the security of software products in general. Of those that gave an answer, only one thought that customers take security of their everyday software products seriously, and two felt that many think security is self-evident and not something that they need to be concerned about.

When discussing the customer's attitudes towards their own products, most of the participants felt that their customers are very demanding when it comes to the security of their products. Only one participant noted that their end-users do not concern themselves with the security of their product but did note that the IT departments of these end-users do handle security seriously.

Table 14. Customer attitudes on security of software products

Own product / Software in general	Attitude	No. of responses
Own product	Demanding	9
	Depending on the product	2
	Not a priority	1
Software in general	Self-evident	2
	Interest is on the rise	1
	Take security seriously	1

"I feel like these customers think its more of a self-evident thing, like they maybe can't experience it, like… how much bad stuff like the software producer can create if they don't take care of the security." (Participant 10)

"They are more critical of our products, because in Finland and I suppose like anywhere, at least, well, probably anywhere in the world, [products and services of a sector] are the kind of a thing that customers need to be able to trust. The whole industry is based on trust so you have to believe that the customers have the kind of an attitude that they count on our products to be secure." (Participant 7)

4.1.11 Additional comments

At the end of the interview, the participants were prompted to consider what had been previously discussed and if they wanted to amend or add anything to their previous answers. The interview participants had varied additional comments, four participants had none and some had extensive additional thoughts and comments arise during the interview. Table 15 shows what themes came up in the comments. The comments could contain more than one theme.

Table 15. Themes in additional comments made by participants

Theme	No. of responses
Testing of software	1
The role of Product Manager	3
Security in the software development process	1
Usable security	1
Security throughout the manufacturing chain	1
Public-private co-operation and rules for secure software	1
Necessary understanding of security for Product Manager	1
Standardization of software security matters and skills	1
Difference between in-house and outsourced software development in context of security and Product Managers	1
Siloed thinking about security in organizations	1
The pace of change in the threat landscape	1
Security as a selling point	1
Different levels of security for different products	1
Process support also for those products where security is not first priority	1
No additional comments	4

“Well, maybe not, I’d like to pinpoint that if we talk about secure software development or product development, so then it [security] is in the center of it and there from the beginning. Like you need to decide in the beginning what level, what needs to be fulfilled and then it goes forward from that.” (Participant 9)

“The question becomes like if we think about the job and the role of a Product Manager, so how knowledgeable and skilful a Product Manager should really be.” (Participant 6)

“Which is okay, but like, maybe in my position I’d like a bit more of having ready processes also for this kind of a more generic product.” (Participant 1)

4.2 Discussion

The primary research question stated in chapter 4.1 was “What is the role of the Product Manager in ensuring the security of software products?” From the interviews, the role can be seen to be an orchestrator role, with a responsibility to see the big picture of the product and to ask, demand or allocate the right things at the right time. The Product Manager was not seen as a role solely responsible for security of the product and the extent of the role the Product Manager has depend on a variety of factors related to the person and the organization.

The role of the Product Manager in general was seen as varying from being very technically oriented to being very business oriented and everything in between. As one interview participant put it: “It’s a multi-talent role, so you need to know a bit about technology, you need to know the business and you need to know about the customer’s industry and also the need.” (Participant 9). According to the interview participants, a Product Manager does not need to have a software developer background, but some idea about how the process works helps. The participants also identified a wide ranging list of responsibilities for the Product Manager in general, in line with the four stereotypical roles put forward in Maglyas et al. (2013), and while exploring the general role of the Product Manager was not within the scope of this work, this ties to the question of what is and is not included within the scope of a Product Manager’s list of responsibilities and why. There did not appear to be a relationship between the security consciousness of the participants’ fields of employments and what they considered to be the responsibilities of Product Managers.

The interviewees approached the issue of software security and the security of software products from the viewpoints of information security on one hand and users on the other. The concepts confidentiality, integrity and availability of information and protection of these were used to define software security, but some participants also approached the issue from the angle of if the user felt the product to be secure. The technicality of the participant’s background did not appear to influence whether they approached the issued from the user point of view or the security of information point of view.

The second research question was “How do Product Managers see their role in the security of software products?” From the interviews we find that the participants saw that they do have a role to play in the matter of the security of their software products. They did not

assign responsibility for the technical details to the Product Manager, but the responsibility to demand for secure implementations and effective security measures was seen to belong to the Product Manager. The Product Manager should know the environment they are operating in, should understand the customer security requirements and ensure that those are met. The interviewees also saw there to be a connection between prioritization decisions and the security of the product.

The third research question was "What are the best tools a Product Manager has for ensuring the security of their software products?" The aim here was to not only gain insight into what kind of means of impacting the security of their software products the Product Managers saw they had at their disposal but to see at which stage of the software development lifecycle they could see having an effect. The toolbox according to the interview participants was varied, however security audits and testing were seen as effective means by the most participants. Considering the literature on the cost of fixing vulnerabilities after deployment, this is something to pay attention to. Some participants were very adamant about the issue; however, it must be noted that the specific wording of the question asked for the best means to ensure security, and security audits can be seen as something that verifies that correct measures have previously been taken. Some participants interpreted the question as the best means to verify the security of the product, whereas others took it to mean best means to ensure the product was secure from the start.

Some participants alighted on tooling and reverse engineering as means to ensure security, which has implications of seeing only the source code and act of writing it as security relevant. This connection was not explored more during interviews. That tooling was bought up here is interesting, however, from the point of view of how widespread their use is. Witchey et el. (2014) looked at reasons why developers are not using the security tools available to them. A newer study from 2020 by Smith et al., focusing on security-oriented static analysis tools and their usability, pointed out that tools are not used due to their usability issues. As one of the interview participants mentioned, the issue of automatic tools should not be a question of costs these days, however they did not consider that their poor usability can and does detract from their use, just as with any other software.

A few participants also mentioned the team and trusting its knowledge on the topic as one of the best means to ensure security in their products. While it is good that the value of trusting the team and listening to their concerns is recognised, as Weir et al. (2021)

encourage developers to approach Product Managers with their security concerns, the flip side to this is the existing research looking at all the ways in which developers do not really think about security (Van der Linden et al. 2020; Xie et al. 2011). Adding to this, thought should be given to how the increasing adoption of low-code/no-code development and self-taught developers can affect the security concerns brought up by the developers. Acar et al. (2017) found that while there are many well covered topics related to software security where support materials are available to developers, they also found that some supporting documents were outdated, or the topic coverage lacked important areas. Thus, while listening to developer concerns is encouraged, relying on the idea that the developers would bring this up if it were a problem is likely to backfire on the Product Manager. Especially if the organizational culture does not encourage this type of communication (Assal & Chiasson 2018).

In terms of terminology and responsibilities in security matters, based on the literature and the interview results presented so far, this work argues the following distinctions. Software security and the security of software products are not the same thing. Software security consists of, as McGrath (2004) defined it, building software that continue to function properly under malicious attack. This entails things like the deployment of correct and effective security features. Security of software products, on the other hand, consists of ensuring that the needs of the user are met so that software security and information security are taken into consideration during the entire lifecycle of the product. Put simply, this entails consideration of the whole picture, including what the correct and effective security features should be.

From the point of view of usable security, the Product Manager is also in a good position to enable the development of products with usable security built into them. Standards and auditing criteria are a good source of hard requirements for security but translating those requirements into product requirements that fulfil the criteria while bearing in mind a realistic take on the risks and maintaining usability is a product management level task. A product can implement highly restrictive security measures, but if the product then becomes unusable or prevents individuals from doing their jobs, it will at best frustrate the people who need the product, and at worst, lead to the users circumventing the security measures in the name of efficiency.

Considering all the various angles pointed out in this work and the existing research into the roles and responsibilities of Product Managers, this work argues for adding security to the admittedly already lengthy list of those responsibilities. The list of responsibilities includes many things the Product Manager is expected to at the least have input on, such as Marketing (Kittlaus, 2022), but which are implemented by other roles within the organization. Why is Marketing included in the list of responsibilities for Product Managers, but Security is not?

There is also an argument for adding security management into the ISPMA SPM framework. As it stands, security management is mentioned nowhere in the framework and considering the increasing importance of security to the long-term viability of software products, its complete omission from a widely accepted framework is glaring. One way to include security management into the framework could be to separate Performance and Risk Management into two core responsibilities for Product Managers, and to add Security in with Risk Management, creating a new Security and Risk Management core responsibility. Another possible way to include security would be to add a new category under the Orchestration umbrella, which would more underline that while Product Managers need to be involved with the security of their product, they are not responsible for the implementation of it.

Whether security is added to a framework or not, Product Managers do themselves a disservice if they leave security up to chance. One interview participant (Participant 12) brought up the data breach of the Finnish online mental health service Vastaamo, for which criminal charges were brought up against not only the perpetrator but also against the then CEO of the company due to failures to protect patient data. The participant posited that if Vastaamo had had a Product Manager, they would likely also have been up against similar charges. A Product Manager who does not recognize their implicit responsibilities for security of their product cannot take the appropriate actions to protect not only their product but also themselves. Despite the dismissive attitudes of some organizations and individuals to software security and the security of software products, in cases of data breaches it is becoming increasingly clear that those in charge of developing said software products cannot make a bona fide claim of not understanding the risks.

In the context of this work, it is worth noting that all the interview participants work in fields where good security practices are essential in the software products that are offered out and that are used in-house. The sample size is also limited, and therefore a wider study of either

a larger sample size of participants with similar profiles or of participants from a wider variety of industries could yield interesting results. Also of interest could be a general look into Product Managers' attitudes to security and comparing those results to the industries they work in. In general, literature looking at security matters from the Product Managers' point of view is hard to find.

5 Conclusions

Software products have reached all facets of modern life, and as such their security has become increasingly important. The costs related to security breaches continue to rise from year to year, and malicious attacks have become a concern to not just large corporations, but small and medium-sized enterprises as well. In a 2023 Forbes article titled “Assessing The Correlation Between Cyber Risk And Business Risk”, David Raissipour notes that the connection between cyber risks and business risks is too evident to no longer be ignored.

This work sought to examine what kind of a role, if any, the Product Managers could have in ensuring that software products are secure, and what kind of means do they have at their disposal in this. Based on the academic and trade literature on product management and software security, there is a role for Product Managers to play when it comes to security but there exists ambiguity as to what that role could be exactly. The predominant framework on software product management does not mention security in any terms.

In addition to a literature review, this work carried out a grounded theory analysis of semi-structured interviews of 13 product management professionals with the aim of understanding how they saw their role in security and what they considered their best means to ensure the security of their products. Based on the interview results, the role was clear to the participants, and they clearly saw for example the connection between their prioritization decisions and the security of their product and understood that they were the ones responsible for security requirements for the products. The best means of ensuring security according to the participants were security audits, penetration tests and testing in general, which was surprising considering that it is relatively well understood that fixing defects after deployment is connected to increased costs.

The interview research for this work was conducted mostly with individuals from organisations that operate in an environment with high security requirements. Considering increasing user demand for security, it would be interesting to conduct a similar interview with individuals from organisations where security is not such a primary requirement.

The interviewees in the interview were Product Managers, Product Owners, or consultants with extensive previous experience from Product Management. A possible future topic for

research could also be how other roles see the Product Manager's role in software security or the security of software products. If for example developer roles do not see there to be a role for Product Managers in anything security related, this would impact how the Product Manager should communicate their security requirements to the development team and how fruitful they could expect discussion to be. Weir et al. (2021) saw positive results from developers engaging with Product Managers on security concerns, could the reversed setting have similarly positive results? A concept discussed in much of literature was the idea of a security champion. This role was often assigned to a member of the development team but looking more widely at what kind of an impact a security conscious Product Manager could have for the general security of software products could also be an area of further study.

An issue that came up in the interviews was finding the appropriate level of security for a given product. To develop further education on the matter, it would be important to understand what Product Managers need to know about security matters to find the correct level for their product.

Based on the literature review and the interviews this work also makes the recommendation to consider including security in the ISPMA-SPM framework, either as a new Security and Risk Management category to the Core SPM activities or as a new Security category in the Orchestration activities.

Too little security is very expensive, as is too much security, just in a different way. It is not necessary to stifle every software product with heavy security measures, but security should be intentional, and someone needs to be able to look at the product and make a deliberate decision about the appropriate level of security for that product. With the insight that a Product Manager should have into the different facets of their product, they are ideally placed to be that person and whether they take the time to consider the security of their product can have far-reaching consequences during the life cycle of the product, for better or for worse.

References

Acar, Y., Stransky, C. Wermke, D. Weir, C., Mazurek, M. & Fahl, S. 2017. 'Developers Need Support, Too: A Survey of Security Advice for Software Developers', in 2017 IEEE Cybersecurity Development (SecDev). [Online]. 2017 IEEE. pp. 22–26.

Albrechtsen, E. 2007. "A Qualitative Study of Users' View on Information Security." Computers & security. [Online]. 26.4 (2007): 276–289.

Anon, J. & González de Villaumbrosia, C. 2017. The Product Book: How to Become a Great Product Manager. [Online]. 2nd ed.

Apunen, A. 2020. Haastajasta hittipalveluksi. 1st ed. Helsinki, Alma Talent.

Assal, H and Chiasson, S. 2018. Security in the software development lifecycle. In Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security (SOUPS '18). [Online]. USENIX Association, USA, 281–296.

Assal, H. & Chiasson, S. 2019. "Think secure from the beginning": A Survey with Software Developers. CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. [Online]. May 2019 Paper No.: 289. Pages 1–13.

Austin, J. 2017. What It Takes to Become a Great Product Manager. [Online]. Available: https://hbr.org/2017/12/what-it-takes-to-become-a-great-product-manager.

Bakker, J. I. (Hans). 2019. "Grounded Theory Methodology and Grounded Theory Method: Introduction to the Special Issue." Sociological focus (Kent, Ohio). [Online]. 52.2 (2019): 91–106.

Banham, R. 2017. Why Cybersecurity Should Be A Nr.1 Priority for 2017. [Online]. Available: https://www.forbes.com/sites/eycybersecurity/2017/03/20/why-cybersecurity-should-be-a-no-1-business-priority-for-2017/#77f0f1bb1719.

Barth, S. & de Jong, M. D. T. 2017. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review." Telematics and informatics. [Online]. 34.7 (2017): 1038–1058.

Buxmann, P., Diefenbach, H. & Hess, T. 2013. The Software Industry Economic Principles, Strategies, Perspectives. [Online]. Berlin, Heidelberg: Springer Berlin Heidelberg.

Caputo, D. D., Pfleeger, S., Sasse, M.A, Ammann, P., Offutt, J. & Deng, L. 2016. Barriers to Usable Security? Three Organizational Case Studies. Vol. 14. [Online]. New York: IEEE.

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J. & Townsend, A. 2020. Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. [Online]. NIST Special Publication 1800-25A. Available: https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html.

The Economist. 2017. Why Everything is Hackable; Computer security. London. Vol. 423. London: The Economist Intelligence Unit N.A., Incorporated.

Elo, S. et al. 2014. Qualitative Content Analysis: A Focus on Trustworthiness. SAGE open. [Online] 4 (1), 215824401452263-.

Emami-Naeini, P., Dixon, H., Agarwal, Y. & Cranor, L. F. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. [Online]. 2019 New York, NY, USA: ACM. pp. 1–12.

Futurice. 2023. Rethinking Product Management. [Online]. Available: https://futurice.com/downloads/en-rethinking-product-management

Goode, S., Lin, C., Tsai, J. C. & Jiang, J. J. 2015. Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers. Decision Support Systems. [Online]. 7073-85.

Haney, J., Acar, Y. & Furman, S. 2021 "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. Proceedings of the 30th USENIX Security Symposium. [Online]. August 11–13.

Heitzenrater, C & Simpson, A. 2016. A Case for the Economics of Secure Software Development. NSPW '16: Proceedings of the 2016 New Security Paradigms Workshop. [Online]. September 2016. Pages 92–105.

IBM. 2025. Cost of a Data Breach Report 2024. [Online]. Available: https://www.ibm.com/reports/data-breach.

Jones, C. 2015. Wastage: The Impact of Poor Quality on Software Economics. Software quality professional. [Online]. 18 (1), 23-.

Kallinen, T. & Kinnunen, T. Etnografia. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto [Online] Available: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/

Kittlaus, H.-B. 2022. Software product management: the ISPMA®-compliant study guide and handbook. Second edition. [Online]. Berlin, Germany: Springer-Verlag GmbH.

Kulyk, O., Milanovic, K. & Pitt, J. 2020. Does My Smart Device Provider Care About My Privacy? Investigating Trust Factors and User Attitudes in IoT Systems, in Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. [Online] 2020 New York, NY, USA: ACM. pp 1-12. Available: https://doi.org/10.1145/3419249.3420108

Kustosch, L., Gañán. C., van 't Schip, M., Eeten, M. V. & Parkin, S. 2023. Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible. Proceedings of the 32nd USENIX Security Symposium. [Online]. August 9–11, 2023.

Maglyas, A. et al. (2013) What are the roles of software product managers? An empirical investigation. The Journal of systems and software. [Online] 86 (12), 3071–3090.

McGraw, G. 2004. Software security. Vol. 2. [Online]. New York: IEEE.

Nina, H., Pow-Sang, J. A. & Villavicencio, M. 2021. Systematic Mapping of the Literature on Secure Software Development. IEEE access. [Online] 936852–36867.

Olama, M. & Nutaro, J. J. 2013. Secure it now or secure it later: The benefits of addressing cybersecurity from the outset, in Proceedings of SPIE - The International Society for Optical Engineering. [Online]. 2013. Proc. of SPIE Vol. 8757.

Raissipour, D. 2023. Assessing The Correlation Between Cyber Risk And Business Risk. Forbes. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2023/06/07/assessing-the-correlation-between-cyber-risk-and-business-risk/.

Ransome, J. F. & Misra, A. 2018. Core software security: Security at the Source. 1st edition. [Online]. United Kingdom: Auerbach Publications.

Rindell, K., Bernsmed, K.& Jaatun, M. G. 2019. Managing Security in Software: Or: How I Learned to Stop Worrying and Manage the Security Technical Debt. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). [Online]. 2019 New York, NY, USA: ACM. pp. 1–8. Available: https://doi.org/10.1145/3339252.3340338

Schwaber, K. & Sutherland, J. 2020. The 2020 Scrum Guide. [Online] Available: https://scrumguides.org/scrum-guide.html.

Smith, J., Quang Do, L. N. & Murphy-Hill, E. 2020. Why Can't Johnny Fix Vulnerabilities: A Usability Evaluation of Static Analysis Tools for Security. In Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security. [Online] August 2020. Article No.: 13. Pages 221–238.

Tkalich, A., Ulfsnes, R. & Brede Moe, N. 2022. Toward an Agile Product Management: What Do Product Managers Do in Agile Companies?. In Agile Processes in Software Engineering and Extreme Programming. [Online] Switzerland: Springer International Publishing AG. p. pp. 168–184. Available: https://doi.org/10.1007/978-3-031-08169-9_ 11

Tøndel, I. A., Soares Cruzes, D., Jaatun, MG & Rindell, K. 2019. The Security Intention Meeting Series as a way to increase visibility of software security decisions in agile development projects. ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security. August 2019Article No.: 59. Pages 1–8. [Online] Available: https://doi.org/10.1145/3339252.3340337.

Tøndel, I. A., Jaatun, M. G. & Soares Cruzes, D. 2020a IT Security Is From Mars, Software Security Is From Venus. Vol. 18. [Online]. IEEE.

Tøndel, I. A., Soares Cruzes, D. & Jaatun, M. G. 2020b. Achieving “Good Enough” Software Security: The Role of Objectivity. In Evaluation and Assessment in Software Engineering (EASE 2020). [Online] 2020 New York, NY, USA: ACM. pp. 360-365. Available: https://doi.org/10.1145/3383219.3383267.

Tøndel, I. A. & Cruzes, D. S. 2022. Continuous software security through security prioritisation meetings. The Journal of systems and software. [Online] 194111477-.

Traficom, 2018. Secure Development – Towards Approval. [Online] Available: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf.

Türpe, S. & Poller, A. 2017. Managing Security Work in Scrum: Tensions and Challenges. In Proceedings of the International Workshop on Secure Software Engineering in DevOps and Agile Development (SecSE 2017). [Online] Available: https://ceur-ws.org/Vol-1977/paper4.pdf.

van der Linden, D., Anthonysamy, P., Nuseibeh, B, Tun, T. T., Petre, M., Levine, M., Towse, J. & Rashid, A. 2020. 'Schrödinger's Security: Opening the Box on App Developers' Security Rationale', in 2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE). [Online]. 2020 ACM. pp. 149–160. Available: https://doi.org/l0.1145/3377811.3380394.

Venson, E., Guo, X., Yan, Z. & Boehm, B. 2019. Costing Secure Software Development – A Systematic Mapping Study. In Proceedings of the 14th International Conference on Availability, Reliability and Security. [Online]. 2019 New York, NY, USA: ACM. pp. 1–11.

Venson, E., Clark, B. & Boehm, B. 2024. The effects of required security on software development effort. The Journal of systems and software. [Online] 207111874-.

Weir, C., Migues, S., Ware, M. & Williams, L. 2021. Infiltrating security into development: exploring the world's largest software security study. In Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. [Online]. 2021 New York, NY, USA: ACM. pp. 1326–1336. Available: https://dl.acm.org/doi/abs/10.1145/3468264.3473926.

Weir, C., Becker, I. & Blair, L. 2021a. A Passion for Security: Intervening to Help Software Developers. In 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). [Online]. 2021 Piscataway, NJ, USA: IEEE Press. pp. 21–30.

Weir, C., Becker, I. & Blair, L. 2022. Incorporating software security: using developer workshops to engage product managers. Empirical software engineering: an international journal. [Online] 28 (2), 21-.

Xie, J., Lipford, H. R. & Chu, B. 2011. Why do programmers make security errors?. In 2011 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC). [Online]. 2011 IEEE. pp. 161–164.

Appendix 1. Interview questions

Background information/individual:

- Educational background?

- Previous work and current position?

- Years of experience working in product management?

Background information/organization:

- Briefly describe your organization and the product(s) you work with?

- What is the role of Product Manager like in your organization?

- Does your organization implement some specific framework for product management?

- What are your main responsibilities as a Product Manager/Product Owner?

- What is your level of involvement in software development? What kinds of things do you make decisions about?

Specific information relating to PM/PO and the security of software products:

- Define “security of software products” or “software security”?

- Whose responsibility is the security of a software product?

- Does the PM/PO have any role in ensuring software security?

    - o What kind?

    - o If no, why not?

- Which of your decisions have implications to the security of your product(s)?

    - o Why?

- How much does security play into your priorities when making decisions about development and maintenance of a product?

- When would you prioritize security?

- What do you think are your best means of ensuring the security of your product(s)?

o Why?

Organizational attitude to security:

- How does your organization handle software security? How do you ensure the security of your products?

- Does your organization have a dedicated information security unit? What is their role like?

- What is your customers' attitude towards software security?

    o Software products in general?

    o The software products you offer?

Finalize:

- Anything to add to previous thoughts?