Simo Leinonen

PASSWORD MANAGER SELECTION IN ORGANIZATIONS

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2021

ABSTRACT

Leinonen, Simo
Password manager selection in organizations
Jyväskylä: University of Jyväskylä, 2021, 64 pp.
Information Systems, Master's Thesis
Supervisor(s): Woods, Naomi

Password managers are commonly recognized as effective and useful tools by cyber security experts that bolster the all-around security of those that utilize them. Password managers provide significant benefits to its users from both security and usability standpoints. Both organizations and individuals alike use password managers as part of their daily lives. However, little knowledge exists on how organizations should go about selecting the appropriate password manager product, which can be challenging due to a saturated market of seemingly similar products. The aim of this thesis is to shed light on the selection process of password managers in organizations in order to highlight important themes and factors for organizations planning to make such a decision. The thesis also dives into the topic of organizational software selection processes in order to support and understand the examination of the password manager selection process. This study contributes to the body of existing password manager literature by combining the findings of a literature review and the results of an empirical research process in order to answer a research question that is intended to fill a gap in password manager research. The results implicate that the usability and security of password managers are imperative criteria for the successful adoption and selection of such a product. The results also indicate that industry practitioners are generally aware of the most important aspects of password manager products as well as their common shortcomings and challenges of their usage within organizations. These results fill a gap in existing password manager research and offer valuable insight for future research as well as industry practitioners.

Keywords: passwords, password manager, software selection, software procurement

TIIVISTELMÄ

Leinonen, Simo
Salasanaohjelmistojen valinta organisaatioissa
Jyväskylä: Jyväskylän yliopisto, 2021, 64 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Woods, Naomi

Salasanojen hallintajärjestelmät tai ohjelmistot ovat yleisesti tunnistettu tehokkaina ja hyödyllisinä työkaluina, jotka vahvistavat niiden käyttäjien kokonaisvaltaista turvallisuutta. Salasanojen hallintajärjestelmät tarjoavat käyttäjilleen huomattavia hyötyjä sekä turvallisuuden että käytettävyyden saralla. Sekä organisaatiot että yksilöt käyttävät salasanojen hallintajärjestelmiä osana heidän päivittäistä elämäänsä. Tästä huolimatta siitä prosessista miten organisaatioiden tulisi menetellä salasanojen hallintajärjestelmiä valittaessa on hyvin vähän tietoa, joka voi olla haastavaa johtuen saturoituneesta markkinasta, joka on täynnä toisiaan näennäisesti muistuttavia tuotteita. Tämän pro gradu tutkielman tarkoituksena on tutkia salasanojen hallintajärjestelmien valintaprosessia organisaatioissa, jotta voidaan tuoda esiin siihen liittyviä tärkeitä teemoja niitä organisaatioita varten, joiden tavoitteena on tehdä tällainen valinta. Tutkielma käsittelee myös ohjelmistojen valintamenetelmiä organisaatioissa, jotta voitaisiin tukea ja ymmärtää salasanojen hallintajärjestelmien valintamenetelmiä. Tämä pro gradu tutkielma rakentaa olemassa olevan salasanojen hallintajärjestelmäkirjallisuuden jatkeeksi yhdistelemällä kirjallisuuskatsauksen sekä empiirisen tutkimuksen löydökset. Sekä kirjallisuuskatsauksen sekä empiirisen tutkimuksen tulokset indikoivat että käytettävyys sekä tietoturvallisuus ovat ensisijaisen tärkeitä kriteerejä salasanojen hallintajärjestelmiä valittaessa. Tulokset kertovat myös, että alan ammattilaiset ovat yleisesti tietoisia salasanojen hallintajärjestelmien tärkeimmistä osapuolista, sekä myös niiden yleisimmistä heikkouksista ja käytön haasteista heidän organisaatioissaan. Nämä tulokset täyttävät aukon tutkimuksessa salasanojen hallintajärjestelmiin liittyen, sekä tarjoavat arvokkaita näkökulmia tulevan tutkimuksen sekä alan ammattilaisille.

Avainsanat: salasanat, salasanojen hallintajärjestelmät, ohjelmistojen valinta, ohjelmistojen valintamenettely

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

At this point of time passwords are still one of the most ubiquitous ways for a user to authenticate themselves when accessing an information system, software, website, or any service or device deemed important enough to warrant some type of access control. Even though many supporting technologies, processes, and strategies of varying effectiveness and success have been introduced, nothing changes the fact that in the end passwords are still merely strings of alphanumeric characters and are thus vulnerable to misuse. Password manager products have been introduced as one way to mitigate the risks related to various challenges and issues that password authentication causes.

A wide variety of different types of systems and technologies exist that either reduce the number of passwords that a user needs to memorize or eliminate the need for entering passwords all together. However, not every system that uses password authentication can implement alternative authentication technologies. This is especially true within the corporate world, where organizations utilize a wide portfolio of different types of software from varying number of vendors. This issue of several different systems and associated accounts is significant and introduces the need for password manager software. Password managers are software products that allow its users to save passwords in a single place to reuse them repeatedly without having to specifically to remember them (Huth, Orlando & Pesante, 2012). Password manager products are said to ease the memory strain of users by eliminating the need to remember a significant amount of different unique passwords (McCarney, 2013). Additionally, password managers make it possible to use complex unpredictable passwords that enhance the security of the user but that are hard for humans to remember (Karole, Saxena & Christin, 2010).

However, adopting a password manager product into use in an organization cannot be done on a whim. Problems arise due to the fact that the market of password manager products is crowded by seemingly identical products with similar sets of features (Walkup, 2016). If an organization decides to start utilizing password managers as part of their daily operations, they also need to make

sure that they avoid the potential pitfalls of selecting the inferior product. The selection bears great significance, as selecting the wrong product could mean a product with significant security flaws or poor usability (Gasti & Rasmussen, 2012; Silver at al., 2014; Zhao, Yue & Sun, 2013). What drives the selection process of password manager products and which criteria do IT decision makers focus on when attempting to select the most suitable password manager? So far, the question of how organizations determine which password manager to select into their organization has not been answered in previous research.

The purpose of this thesis is to study and examine the selection process of password manager software in organizations. To achieve this the following research question will be answered as a part of this thesis: What are the most important criteria when selecting a password manager software product? To be able to answer to the research question a literature review on password managers will be conducted as a part of this thesis. The literature review will study the results of existing academic literature relating to password managers and its various aspects. To examine the validity of the results of the literature review and to test its theories, an empirical research process will be conducted to study both the accuracy of academical papers and studies, as well as how the phenomenon of selecting password manager products in organizations is facilitated. The empirical research will be conducted through a series of qualitative interviews in order to extract empirical data on how password manager products are selected and evaluated in organizations.

In addition to the above-mentioned topics and to support the examination of password manager selection processes, literature review into software selection methods and theories will be carried out during this thesis. The purpose of examining software selecting methods and theories during both the literature review and the empirical research process is to better understand how software products are selected and evaluated in general. This baseline understanding will aid in the examination of password manager selection processes. To support the main research question the following supporting research question is formulated: Do the selection criteria for password managers significantly differ from selection criteria of software products in general? In addition to this, the following research question will be answered to examine the findings of the literature review and empirical research: Can generic software selection criteria be defined?

The structure of this thesis is the following. A literature review will be conducted in the next chapter that will detail the existing academic research on the topics of password managers and software selection methods. The findings and theories of the literature review will be summarized in the theoretical framework chapter. The theories and findings of the literature review will guide the formulation of the empirical research, which will be detailed in the empirical research design chapter. The results of the empirical research will be elaborated on in the empirical research results chapter. The discussion chapter will tie the findings of the literature review and the empirical research process together by providing conclusions and answers the research questions of this

thesis. Limitations, implications for practice and research, and future research suggestions will also be detailed in this chapter. The thesis will be concluded by a summary chapter that will detail the findings of this thesis in a concise manner.

2 Passwords & password manager software

This chapter contains the literature review portion of this master's thesis. It will cover the current knowledge of passwords and password authentication, password manager software, software selection processes and other concepts that are relevant for the topic of the empirical research portion of this thesis.

2.1 Passwords

Passwords are the most common way for users to authenticate their identity to access information systems and other IT services such as websites, applications, online accounts, databases, physical devices and many others (McCarney, Barrera, Clark, Chiasson & Van Oorschot, 2012; Zhao & Yue, 2014). The fundamental idea of passwords is to ask the authenticating user for something only they know. By asking for something only the specific user knows should in theory stop misuse of these password restricted services.

However, the real world and its numerous complexities deteriorate the reliability of password authentication methods. In a vacuum, a password system is a rather good way to authenticate users, but practical problems, humane error, and other reasons present a real challenge to their resiliency.

2.1.1 Strengths of password authentication

Regardless of the critique passwords have received for several decades now, the technology possesses some inherent benefits that have made the authentication method as prevalent as it is. Despite decades of suggestions and research from academia and security experts, no viable or wide-spread solutions have yet been found (Herley & Van Oorschot, 2011; Bonneau, et al., 2012). This is due to both password authentication's good features, as well as the difficulty of developing a viable new authentication technology that could be as easily deployed and learned as current password authentication methods.

As concluded by Herley & Van Oorschot (2011), password authentication method has actually been the single best solution out of all existing authentication methods regardless of the technology's multiple faults and shortcomings. Some reasons for the prevalence of password authentication include its simple technical setup, easy user administration, simple usability, existing general knowledge among users, and the fact that their usage is not tied to a physical artefact or a location (Herley & Van Oorschot, 2011).

Besides technical and organizational issues, social and human factors also play a role in the persistence of password authentication technology. In previous research, it is commonly understood that increasing information security via new organizational security policies or introducing other security measures has a heavy impact on usability and the desire to use the underlying technology. (Arias-Cabarcos et al., 2016; Karole et al., 2010; Dhamija & Dusseault, 2008)

Because of the fact that passwords present a rather viable solution for user authentication at the moment, it is even harder for newer more secure authentication methods to arise. Alternative authentication methods have not so far become more than curiosities in the broader scheme of online user authentication (Herley & Van Oorschot, 2011). A large part of the reason for why passwords have not yet been replaces by something more secure is the fact that alternative technologies and systems are simply too difficult and expensive to setup and adopt (Bonneau et al., 2012; Ives et al., 2004). Added security measures have just not proved to be worth of the investment and higher costs on a global scale thus far. Besides high costs and technical limitations, Herley, Van Oorschot and Patrick (2009) list many reasons for why the IT world has not yet been able to move past including convoluted authentication technology landscape, organizational competition, and the lack of a centralized force that could impose such a change.

2.1.2 Issues with password authentication

Even though passwords are still ubiquitous in combination with most online services, they have received a significant amount of justified critique over the years. The critique has come from all sides: users, academia, security experts, and industry practitioners. The issues of password authentication are multitudinous. Technological vulnerabilities, social issues, policy related issues, user habits and others all plague the integrity of these authentication systems. (Zhao & Yue, 2014; Stober & Biddle, 2015; Wash, Rader, Berman & Wellmer, 2016; Choong & Theofanos, 2015; Summers & Bosworth, 2004; Walkup, 2016; Komanduri et al., 2011.)

Many technological security issues exist with password technologies. Prevalent examples of these include SQL injection attacks, brute force attacks, dictionary attacks and many more (Summers & Bosworth, 2004). These attacks are so successful because of the fact that once revealed, passwords are not tied to any physical place, person, device or any other artefact; they can be used at will in many systems without permission. Once stolen, the breached password becomes useless, and the sensitive data protected by the password authentica-

tion scheme can now be considered to be compromised. These breached password databases are most often sold or listed online for anyone willing to see them. This poses a significant risk for that significant number of users who reuse their password across several different services. (Ives, Walsh & Schneider, 2004.)

User habits and social issues also pose a serious security issue for systems with password authentication. Without any education or prior knowledge users tend to set themselves weak passwords, which is a widespread problem amongst internet users (Wash et al., 2016). Due to the ever-rising amount of password secured services another issue beyond just weak passwords has started to arise. Users with a large number of unique services that need their own password tend to drive users to reuse the same passwords across many sites and services (Wash et al., 2016; Grawemeyer & Johnson, 2011). This behavior is also very detrimental to the user's online security. In the case of reusing passwords, an attacker only needs access to one password database that has been setup incorrectly. Once the password and user data has been extracted from the compromised service, especially password reusing users are at risk of having their other accounts compromised (Ives et al., 2004).

Organizations as well as many internet services have started requiring users to set passwords that meet a certain set of complexity requirements. These requirements are a part of the organization security and password policies. These policies' purpose is to set limit to acceptable user behavior in reference to the organizations IT resources (Komanduri et al., 2011). These policies' ultimate goal is protecting the organization and the user, but they can however have a detrimental effect on users' password behavior. Especially password policies that are too demanding and difficult can cause the users of the system users to start adopting insecure password habits such as password re-use (Summers & Bosworth, 2004). This can lead to either reusing the same password with small predictable changes or even writing them down in plaintext. These types of harmful password creation strategies that can be a result of complex organizational password policies are referred to as coping strategies (Inglesant & Sasse, 2010).

2.1.3 Alternatives to password authentication

Alternatives to traditional alphanumeric password authentication methods have been studied for several decades without any significant developments or emergence of a clear new replacement (Herley & Van Oorschot, 2011). Even though no widespread technologies or universally applied solutions have been found by security researchers or practitioners, some prominent technologies that at the very least improve the security of password authentication do exist. The purpose of these alternatives is to provide potential solutions to the issues detailed in the previous chapter.

One generic concept that has made rounds in especially academia is the concept of graphical passwords. Graphical passwords have however not gained

nay significant traction in practice for either consumer or organizational users. The fundamental idea of graphical passwords is that instead of trying to remember a text-based password string the user would setup and authenticate by using a graphical method. (Davis, Monrose & Reiter, 2004; Suo, Zhu & Owen, 2005.)

Two-factor authentication (2FA) is an additional layer of security that has been added to password authentication systems. 2FA's essential idea is that besides asking for something the user know, being the password, the system also requires secondary authentication in order to access the system. Typically, the additional authentication feature is either "something the user has" or "something the user is". (Aloul, Zahidi & El-Hajj, 2009.)

"Something the user has" usually refers to a separate physical token that the authenticating user has on their person (Aloul et al., 2009). In addition to typing in the password, whoever tries to access the system will also need to provide secondary authentication with this physical token in order to access the system. Thus, if the party trying access the system is fraudulent in nature, the attempted system access will be denied if they cannot present the physical artefact upon authenticating to the system. In most cases this physical token is either a smart-device or a token in the shape of a USB-key or an identification card.

"Something the user is" refers to the physical and biometric features of a person which can be used to confirm that the person attempting to authenticate into a system is indeed the correct user (Aloul et al., 2009). These biometric features need to be individual and unique to a single person so nobody can falsify or pretend to be that user. Typical biometric 2FA methods include fingerprints. Less widespread but still existing methods are also iris and facial recognition, even though the former has become more common with new smartphone technologies.

Many organizational usages for 2FA exist and the method is more widespread in an organizational environment. However, many consumer systems and services also offer 2FA authentication for their users, such as Google and Microsoft who provide important and extremely popular online services such as email, productivity tools, cloud storage, platforms, marketplaces and many others. However, overall 2FA seems to gain more popularity among organizational and expert users than people who are not well versed in IT security concepts (Ion, Reeder & Consolvo, 2015).

Single Sign-On (SSO) technologies are also another way to ease the memory load and security issues of password authentication where every system has its own password. Typically, SSO systems are utilized in organizational environments with large portfolios of different organizational services. Essentially SSO methods make it possible for the user to use only one account and password to authenticate into several different services at once. This is in comparison to an environment in which the user would have to have a separate account and a password for each unique service. (Pashalidis & Mitchell, 2003; De Clercq, 2002.)

2.2 Password manager software

If the challenge of phasing out passwords and introducing something else is overwhelming and no immediate relief to the issue is in sight, password managers could significantly improve the current state of affairs when it comes to password authentication.

Many factors in existing research suggest that password managers could be a viable solution to many of the issues password authentication introduces to users and systems (Silver et al., 2014; Arias-Cabarcos et al., 2016). Password managers relief the need for users to remember multiple different passwords; this reduces harmful behavior in terms of password reuse, and writing down passwords (Gray, Franqueira & Yu, 2016). Password managers also make it easy to create, store, and use complex passwords that are outside the grasp of dictionary attacks or social engineering. (Zhao, Yue & Sun, 2013; Alkaldi & Renaud, 2016.)

Password managers do not by any means present an end-all-be-all solution in terms of online authentication methods and their future, but they can provide significant improvements to password-based authentication methods by improving their safety and usability. Password managers can be thus utilized in minimizing and even eliminating some security threats that target password authentication and its shortcomings as their attack vector. (Zhao & Yue, 2014; Stobert & Biddle, 2015; Walkup, 2016.)

2.2.1 Different types of password manager software

Many different types of password managers exist in the market currently. They have different security implementations, feature sets, user interfaces, and fundamental functionality (McCarney et al., 2012; Karole et al., 2010; Gray et al., 2016; Zhao et al., 2013; Alkaldi & Renaud, 2019; Arias-Cabarcos et al., 2016; Luevanos, Elizarras, Hirschi & Yeh, 2017; Zhao et al., 2013; Chiasson, Van Oorschot & Biddle, 2006; Alkaldi & Renaud, 2016).

What all password managers have in common however is the fact that they are used to store password and account information centrally in one single location. This central password storage place is typically secured with a highly secure, complex and long master password. The data behind the password is most often encrypted. Sometimes other additional authentication methods to access the password manager exist on top the master password. (Huth et al., 2012; Stobert & Biddle, 2015)

Password managers can be divided into at least three general categories; local managers, cloud-based managers, and browser managers. Local password managers store all data locally on a device that the user has designated to be

used as the password storage device (Karole et al., 2010; Gray et al., 2016). This means the passwords that the user wishes to save to be used in their password manager will be saved locally, and never sent to a third-party service for storage. One other general type of password managers are cloud-based password managers, in which the password data that the password manager user saves will also be sent to the service provider to be hosted on remote site (Gray et al., 2016). Browser-based password managers are commonly used password managers that are integrated in the most popular web-browser applications such as Google Chrome and Mozilla Firefox (Gray et al., 2016; Zhao & Yue, 2014). All of these implementations have their positives and negatives. A brief overview into password manager literature and a taxonomy different types of password managers can be found in Table 1 at the end of this subchapter.

Local password managers offer the user full control over their own data and how they wish to store it. The user can choose to use a hard-drive, USB-stick or some other physical storage device as their password manager. This way the user never has to relinquish control of their data over to third parties. Regardless of this control, it has been proven that local password managers also suffer from various security issues (Gasti & Rasmussen, 2012; Gray et al., 2016). On the other hand, this control could also be seen as a negative, as the user themselves is responsible for backups and contingency of the password manager program in the case of a hardware failure. Local password managers can also be considered to have lackluster usability due to its inflexibility and lack of portability. (Karole et al., 2010.)

Cloud-based password managers have the major benefit of mobility and ease of access. By saving password data to the cloud, user can utilize the password manager regardless of the device or physical location. Cloud-based managers however present a clear risk as well; in order to achieve the convenience of having access to your passwords anywhere you go, one has to in a sense relinquish control of their passwords and accounts to a third-party. This has been proven to make many users uneasy about using these types of password managers. (Karole et al., 2010.)

Browser-based password managers are the one of the more commonly used managers and for a good reason; they are integrated right into the very tool most people utilize to access online services, a web-browser. These tools are extremely useful and convenient, as they do not require setting up another program just for password management. However, studies have pointed out that many browser-based managers have serious security flaws (Zhao et al., 2013). Besides just native password managers offered by browser vendors, many third-party password manager vendors offer browser plugins with their applications that allows the third-party programs to function alike native browser-based password managers.

TABLE 1 Different types of password managers in literature

Local password managers	Karole et al., (2010); Gasti & Rasmussen (2012); Gray et al., (2016); Arias-Cabaros et al., (2016); Luevanos et al., (2017)
Cloud-based managers	Karole et al., (2010); Gasti & Rasmussen (2012); Gray et al., (2016); Zhao et al., (2013); Arias-Cabaros et al., (2016); Luevanos et al., (2017)
Browser managers	Zhao & Yue (2014); Gray et al., (2016) Zhao et al., (2013); Alkaldi & Renaud (2019); Walkup, (2016); Arias-Cabaros et al., (2016); Luevanos et al., (2017)
Other manager types (Portable, Hybrid, Stand-alone)	Karole et al., (2010); Alkaldi & Renaud (2019); Chiasson et al., (2006)

2.2.2 Password manager usage positives

Password managers are generally regarded by experts as one of the best ways to reduce the risks involved with password authentication systems and technologies (Ion et al., 2015; Silver et al., 2014; Huth et al., 2012). This is because password managers and their usage can yield their users many security benefits. The fact that password managers make it possible for the user to create highly secure, unique, and complex passwords for each and every service they utilize is the greatest benefit of their existence. These factors alone work as a deterrence and defense against various attacks targeting user password usage and online authentication, such as dictionary and brute force attacks. (Zhao & Yue, 2014; Silver et al., 2014.)

Using password managers also reduces memory burden for their users. Bad password habits such as reusage and weak passwords are sometimes induced by the sheer number of different types of online services and accounts that users need authentication for. Sometimes complicated corporate password policies also drive these bad password habits by being too restrictive and causing high levels of memory burden to users. Regardless of why bad password habits exist, the usage of a password manager reduces the occurrence of these habits, and thus heighten the security level of the individual and the organization they represent. (Stobert & Biddle, 2015; Zhao et al., 2013; Alkaldi & Renaud, 2016.)

2.2.3 Password manager critique

Regardless of their well-documented and studied benefits password managers possess some risks and potential pitfalls. Several studies list negative effects and phenomena that are related to password managers.

Even though password manager usage would be beneficial according to existing research and best practices, it has been determined that users generally are not interested in using a password manager and that adoption rates are low among general internet using population (Alkaldi & Renaud, 2016). One of the main concerns for users is their usability; many users find that using an additional tool for managing password is too complex, bothersome, and time consuming. (Karole, Saxena & Christin, 2010; Aurigemma, Mattson & Leonard, 2017; Fagan, Albayram, Khan & Buck, 2017; Chiasson, van Oorschot & Biddle, 2006.)

In addition to usability issues cited by users there are many other reasons for choosing not to use password managers. A repeating concern for potential users is that users do not feel comfortable surrendering their private passwords to third parties, including password managers (Chiasson et al., 2006; Fagan et al., 2017; Karole et al., 2010). Based on previous research, it seems that users often misunderstand how password managers can improve security and do not understand the operating principle of them. This phenomenon can be interpreted as apathy or even ignorance towards potential password related security risks. (Fagan et al., 2017; Aurigemma et al., 2017.)

Users' security concerns and skepticism are not unfounded however, as password manager vendors and specific products have also received critique due to their lacking security, faulty implementation, or misconfigured applications that have the potential to reveal user data to attackers. Some studies have found that despite advertising to be a secure way to store user's data, the tools sometimes present some serious security risks that potential attackers could take advantage of. (McCarney et al., 2012; Gasti & Rasmussen, 2012; Silver et al., 2014; Zhao et al., 2013.) As Gasti and Rasmussen (2012) elaborate in their study, many of the examined password manager tools were found to have lacking and insufficient protections against even basic attacks. If conducted by a malicious attacker, an attack would have rendered these password managers useless and pose a highly dangerous security issue. Several different types of vulnerabilities concerning encryption protocols, network protocols, different attack vectors, and others were uncovered in the study by Zhao et al. (2013).

2.2.4 Summary of password managers

There is seemingly no common consensus over the usage of password manager programs; while many studies seem to regard password managers as overall good tools and think they can relieve some fundamental issues that current password authentication schemes present, some still consider them a temporary patch to a bigger issue that needs addressing urgently. However, it can be gen-

eralized that password managers are viewed mostly favorably and as an easy way to secure oneself better in the world of endless online services and password policies (Zhao & Yue, 2014; Silver et al., 2014; Ion et al., 2015).

One topic that constantly arises in relevant literature in combination with additional security features is the topic of usability. Researchers seem to reach similar conclusions repeatedly; usability and user friendliness are essential for the widespread adoption of any new authentication related technology. Users are reluctant to adopt new security measures even though they are aware of the risks they face by omitting the usage of such technologies. This reluctance is often also extended to the adoption and low usage rates of password managers.

Another concept that can be found in literature on several occasion are user misconceptions about the purpose, function, and usage of password managers. Generally, users do not seem to understand the underlaying principle behind the aforementioned tools, and thus do not seem to often exhibit any interest in using a such tool voluntarily.

Besides having apathy over the benefits of password manager tools, users also display that they are not aware of the security risks presented by the various threats that target online user authentication methods such as passwords. Users are also often dubious of surrendering their most important and critical credentials to the hands of third parties. This notion of lack of trust is however not totally unrealistic, as one unfortunate discovery from relevant literature is the fact that many password manager applications seem to have considerable security flaws. The combination of these above factors severely hinders the widespread popularity of password manager tools, and they should be addressed by IT experts, organizations, and password manager vendors before these tools can become more popular over the general populace.

As a concluding remark about password managers it could be said that they do not by any means fully solve the fundamental issues password authentication presents. However, as stated earlier, password managers can significantly reduce or even eliminate some security threats related to password authentication methods, and are thus worthy of at least considering for any and all organization and individuals who use and struggle with online services and the password management issue that comes along with them.

3 Software procurement and selection

This chapter will elaborate on the concepts of software procurement and selection in organizations. The purpose of this study is to examine the phenomenon of how and why password manager products are selected in organizations. As password managers are software products like any other, their selection also follows some kind of a software procurement process within an organization. Therefore, in order to understand how password manager products are selected in organizations one must also understand the dynamics and general theory of software procurement and selection. If these concepts are not understood, it becomes difficult to evaluate the selection process of password managers in organizations.

The following chapter and its subsections will detail how the process of software procurement and selection function in organizations. Firstly, the concepts of outsourcing and software procurement in organizations will be examined in order to lay the foundation on how organizations acquire software products from third parties. Secondly, a review on some notable software evaluation and selection models will be detailed. Lastly, the chapter will include sections on how these third-party products are evaluated and selected by utilizing series of different criteria.

Software procurement refers to the process of acquiring software products from outside the organization into the usage of the organization. Usually software is procured from third party providers and vendors. The purpose of software procurement from third party providers and vendors is to compliment some business function or process by utilizing some type of software to aid the organization to reach its objectives (Gonzales, Gasco & Llopis, 2010).

As information systems and software products are the very foundation of businesses and their critical functions, the software procurement process has become a key issue when it comes to the success of the whole organization (Stefanou, 2000). A wrong decision regarding the acquirement of software products can prove to be quite costly in terms of operating costs, as well as the bottom line in a worst-case scenario. Inversely, a successful software acquirement and procurement project can have a significant positive reaction to the

organization's operations and financial well-being. (Jadhav & Sonar, 2009; Clemons & Chen, 2011.)

Badampudi, Wohlin and Petersen (2016) elaborate on different ways software developers can source software components to be used in their own development efforts. Even though the article in question focuses on software development, the basic principle can be generalized into IT service management in which complete software packages and products are often purchased. Badampudi et al. (2016) see that software sourcing can be done from four different sources: from within the same organization, bought from the market, open-source software acquired for free, and outsourcing the development of the needed software.

Hackman (2003) presents a more generic model of IT and software procurement in their article. The text emphasizes how complicated the process of software procurement can really be, as according to Hackman (2003) the process is both interdisciplinary within the procuring organization, as well as convoluted when it comes to the software market and its wide variety of product offerings.

Regardless of the type of software being procured into the use of the organization, the fundamental idea remains the same; a vast amount of different types of software products exist for any specific use case an organization might encounter. Therefore, the selection of the correct product can prove to be quite challenging and sometimes daunting task due to the combination of abundance of seemingly similar products as well as the potential magnitude of the procurement selection. The following subchapters will examine outsourcing of IT, software selection processes, software selection models, and software selection criteria.

3.1 Outsourcing of IT

As the procurement of software most often refers to the process of acquiring software resources from third parties outside of the organization, it is fair to draw some comparisons between software procurement activities and the general concept of business outsourcing (Clemons & Chen, 2011). By definition, outsourcing refers to the process where an organization or an individual purchases work, labor, or services from a third-party provider (Cambridge English Dictionary, 2019). Outsourcing is a common theme in the manufacturing of physical goods and fulfillment of many professional services in the world of commerce. Oftentimes the concept of outsourcing is done to save costs, simplify organizational goals and structure, focus on main tasks, and other reasons.

These same concepts and reasons can be stretched to fit IT functions and services, which have been also outsourced for some time now. This process can also be referred to as IT outsourcing. The fundamental logic in the outsourcing of IT activities is the same as for any other business function; save money and to

achieve organizational and processional benefits. (Dibbern, Goles, Hirschheim & Jayatilaka, 2004.)

Outsourcing in the realm of IT can be done both through as buying some continuing service from a third-party service provider, or by buying individual efforts such as the development of some custom software component. One of the more popular methods of IT outsourcing is the Software-as-a-Service (SaaS) method, in which software resources and computing services are bought from an external service provider (Ma, 2007; Clemons & Chen, 2011). Another concept for acquiring software products from outside the organization is the Commercial-Off-The-Shelf (COTS) method, in which ready software packages or components are purchased from the market from third party software vendors (Lin, Lai, Ullrich, Kuca, McClelland, Shaffer-Gant, Pacheco, Dalton & Watkins, 2007). Regardless of what services or products are being purchased, the fact is that these services are being purchased from outside of the organization, in comparison to them being built in-house.

McFarlan and Nolan (1995) elaborate about various aspects of IT outsourcing and its challenges and concepts in their research. As a part of their research, they introduce a strategic grid model that details general situations in which IT outsourcing may or may not be beneficial for the organization. In a summarizing fashion it could be stated that IT functions that involve high level of innovation are generally better off being kept in-house. And inversely IT functions that are less advanced and innovative in nature should generally be outsourced to third party providers. (McFarlan & Nolan, 1995.)

3.2 Software selection process in organizations

The process of selecting new software can be extremely convoluted depending on what type of a software product the organization is looking for. Some business functions or applications have dozens or hundreds of different types of unique software solutions to choose from. The number of seemingly similar options can make the task of choosing the right application rather challenging. (Marr & Neely, 2003; Repschlaeger, Wind, Zarnekow & Turowski, 2012; Arditi & Singh, 1991.)

It seems that the concept of IT procurement process is also rather understudied, and it is difficult to find enough academic literature on the subject to form comprehensive theories regarding this subject. Both Badampudi et al. (2016) and Heckman (1999) implicate in their texts that there is a lack of literature and studies about the process of IT procurement and sourcing software from outside the organization. Neither generic or comprehensive models regarding software selection really exist, and there is no currently available list of software selection criteria. This means industry practitioners often have to rely on inaccurate and unsuitable selection criteria as a part of their software selection and acquisition process. (Keil & Tiwana, 2006; Jadhav & Sonar, 2009.)

These factors can make the challenge of choosing the one correct product quite daunting for IT and business decision makers. Additional factors such as the amount of resources committed to the acquirement of the new software, the price of implementation, training, degree of business criticality and importance for core business functions can heighten the difficulty of choosing the right software for the needs of the organization. (Arditi & Singh, 1991.)

3.3 Software selection models in literature

The concept of software selection methods and their usage in empirical contexts has been studied in numerous different studies and previous research. Some of these studies have explored the utilization of older models that have been modified to fit the purposes of selecting software products, while some have chosen to introduce completely new models and frameworks on the process of software selection (Tam & Tummala, 2001; Alanbay, 2005; Goodhue & Thompson, 1995; Heckman, 1999). Some of these models will be presented in the following subchapter to provide an overview on how academia sees the process of software selection and how the phenomenon can be quantified and studied.

The Technology-Organization-Environment (TOE) model is a model that examines the adoption of technology in an organizational context. Its purpose is to elaborate how the three aspects of the TOE model affect the utilization and usage of new technologies. (Oliviera & Martins, 2010.)

While the TOE model is more concerned about the adoption of new technology innovations into organizations, it could be taken into consideration while attempting to select the software that is the best fit into an organization. Studies have shown that the TOE model can be modified to fit the evaluation and implementation processes of different types of technologies and products (Bradford, Earp & Grapski, 2014). By at least examining what type of a technology would be the best fit with the other two factors of the model, organization and environment, IT managers and organizational decision-makers could enhance their ability to select the right software products for their organization. Many IT employees do not have the influence to change how an entire organization works neither would it be feasible to do so, but instead focusing on attempting to select the best technology for its existing surroundings could possibly yield greater results rather than simply selecting the product that seems to be the best choice in a vacuum.

Heckman (1999) presents a model for the management of the IT procurement process. According to the paper the process of selecting the appropriate software is one subtask of a larger more extensive organizational effort to acquire fitting and effective software into the use of an organization. Heckman (1999) also asserts that the process of IT procurement should be defined, monitored, measured to achieve a greater degree of accuracy and efficiency as well as more successful outcomes. The model and practices that are introduced in

this article could be at the very least evaluated by organizations and managers that are involved in the process of software procurement in their line of work.

Goodhue and Thompson (1995) suggest the Task-Technology-Fit (TTF) model in their research. Its purpose is to examine and elaborate the relationship between technology and the potential positive impact it can have on the operation and performance of the utilizer of the technology, such as the workforce of an organization. In the model's essence is the presumption that a certain type of technology exists for each unique task and use-case that will significantly improve the performance and output of the utilized of the technology (Goodhue & Thompson, 1995). While considering the best possible software to select and acquire into an organization, the decision makers could take the TTF model into consideration. By taking the TTF model into account in software product evaluation processes, decision-makers can make more informed decisions on which software might or might not be the better fit for their specific user needs and use cases in their own organization. The authors also specify that the model could be used to assess the how well a particular technology or a software product suits a particular organization's use case and environment. (Goodhue & Thompson, 1995)

The Analytical Hierarchy Process (AHP) is a multi-criteria selection model that is intended to be utilized in any decision-making process in which there are several options and criteria to be considered. This can be also referred to as multi-criteria decision-making process, in which multiple alternative solutions compete. The AHP was created in the 1980's and 1990's and has been revised and modified in numerous academic studies. (Saaty, 1990; Tam & Tummala, 2001; Davis & Williams, 1994.)

AHP is generic in its essence, meaning it can be modified to be used in any decision-making situation that involves several options to choose from and a set of predetermined criteria. Due to its generic and flexible nature, AHP and its derivatives have been utilized in a large number of software selection and procurement literature as well (Alanbay, 2005; Cheng & Li, 2007; Lai et al., 1999; Ngai & Chan, 2005; Jadhav & Sonar, 2009).

The AHP carries both positive and negative aspects in relation to its practical usage. As stated earlier, AHP is generic in nature and is thus easy to adapt into any multi-criteria decision-making situation. This allows for its utilizer to simply gather requirements after which the model can be used to calculate the best solution out of several options. The negative side of AHP includes the fact that once requirements have been gathered and their relative importance has been calculated, any change into the model requires for the model to be completely recreated. Changes that require for the model to be reconfigured include the selection criteria weights and changing the number of selection criteria. It should also be noted that although the usage of the model itself is simple, the acquirement and evaluation of the necessary criteria and their relative importance can be a challenging process especially for more complex and important systems. AHP can also be used without the relative weights of the competing requirements, but this reduces the accuracy of the model.

Tam and Tummala (2001) have applied the AHP method in their research, in which they studied the usage of AHP as a decision-making component in a real life IS selection process. They applied the AHP method to decide and select a telecommunications system for a telecommunications corporation. The authors of the study felt that AHP is a good tool to utilize as a part of a software selection process. It was noted that AHP presents a way to examine a complex multi-factor decision problem in a systematical way. It was also noted that by using the AHP decision-makers can significantly reduce the time it takes to come to a conclusion about their decision. (Tam & Tummala, 2001.)

Mamaghani (2002) has also conducted research regarding the usage of the AHP model in the selection of software in a real-life organizational context. In their research, an organization applied the AHP model to assist in the selection of antivirus and content filtering software for organizational use. Mamaghani (2002) felt that the AHP model was especially apt in this case due to the sheer number of available software products.

Below is a modified graphical model of the AHP model that has been adapted to a software selection multi-criteria problem.

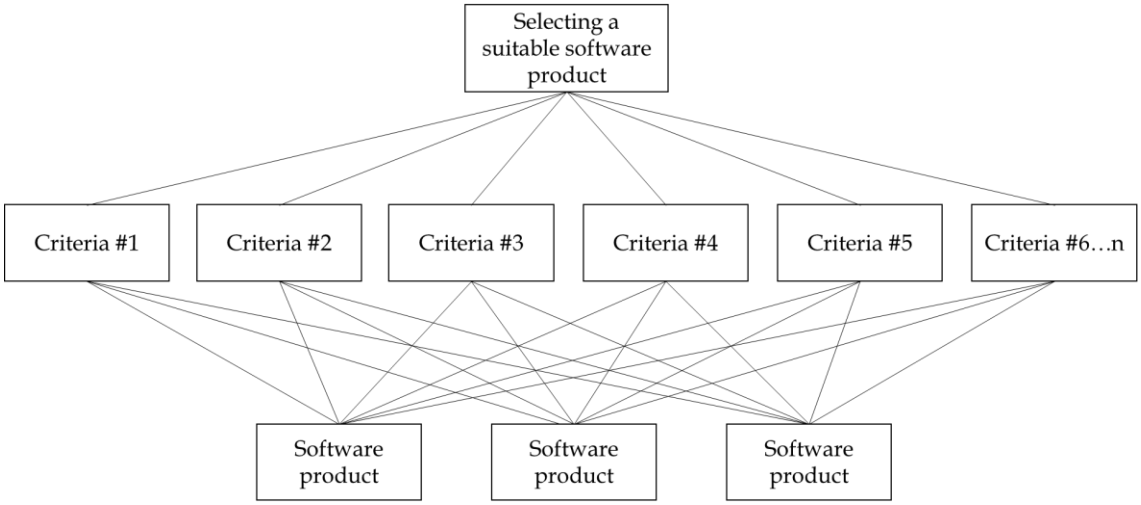

FIGURE 1 A generic adaptation of the AHP model, derived from Saaty (1990), Tam and Tummala (2001), and Mamaghani (2002).

This adaptation of the model presents a very generic theory of how the AHP model could be used as a part of various different types of software selection processes. It has been proposed in literature several times that the AHP model is a useful methodology to consider when dealing with multi-criteria decision-making problems (Alanbay, 2005; Lai, Trueblood & Wong, 1999; Ngai & Chan, 2005; Tam & Tummala, 2001). Of course, in order to use this model efficiently, one would need the specific criteria and candidate software product infor-

mation in order to form weights and levels of importance for different criteria. However, this model presents a generic software selection model that has been derived from the AHP model as stated earlier.

3.4 Acquiring selection criteria

In order to acquire any kind of software into an organization, the organization must first determine the requirements that the new software needs to correspond to. As each organization's requirements, organizational and IT environments, as well as goals are different it is important that each organization considers themselves which software product out on the market would be the best fit to them individually. For example, the purchasing and selection process for smaller organizations is often less complex and nimbler than the similar process for larger organizations (Bernroider & Koch, 2001).

The acquirement and importance of selection criteria is also different depending on what type of software is being acquired. A mission critical and organization wide information system should have a more complex and elaborate list of requirements and selection criteria than a less frequently used support service (Benlian & Hess, 2011).

Acquiring the selection criteria is important due to the fact that in the actual selection or comparison phase these criteria will be used to rank the potential candidates. For example, the Analytical Hierarchy Process (AHP) which is a multi-criteria decision-making model requires a list of the preferred criteria in order to be useful (Lai et al., 1999).

3.5 Software selection criteria in literature

Due to the sheer number of different types of software applications and their unique use cases, each individual software selection process is unique with its own determining and defining factors. However, clear trends about what selection criteria are more common and perhaps thus important for IT and organizational decision-makers can be found in literature examining software selection processes and software selection criteria.

I have examined a set of 15 academic studies that have studied the process of software selection within organizations. In these studies, the set of criteria that was found to be used in the process of selecting software to be adopted by organizations varied wildly. The studies dealt with different types of software including Enterprise Resource Planning (ERP), Cloud Services, Software-as-a-Service (SaaS), auditing, supply chain management, office tools, accounting and others. All of the previously mentioned studies listed or mentioned software selection criteria in some type of fashion within their study.

Even though the studied in question examined different types of software selection projects across various different business areas, some software decision criteria were found to be more significant and prevalent across these studies. Out of the 15 examined articles, four distinct criteria appeared 10 times or more: support & service (13), cost (12), functionality & features (11), and vendor (10). On the contrary, several initially seemingly important selection criteria appeared three times or less: maintenance (3), transparency (3), contract (2), geolocation (2), and legal compliance (2). Several selection criteria that were only mentioned once in the research material were excluded from this analysis as outliers and insignificant factors.

Below you can find the results of the literature review of software selection research articles. In this figure, I have gathered the most commonly found software selection criteria that were mentioned in the underlaying material. Any criterion that was mentioned less than 4 times was eliminated from this figure in order to make it presentable in this thesis format. The criteria listed the following Figure 2 are in order from left to right: Cost, Flexibility, Compatibility/Integration, Customization, Usability & UI & UX, Support & Service, Backups/Continency, Reporting & Analysis & Monitoring & Data, Vendor, Ease of Implementation/Deployment, Security, Functionality/Features, Stability & Availability & Reliability, Scalability, Technical specifications and compatibility.

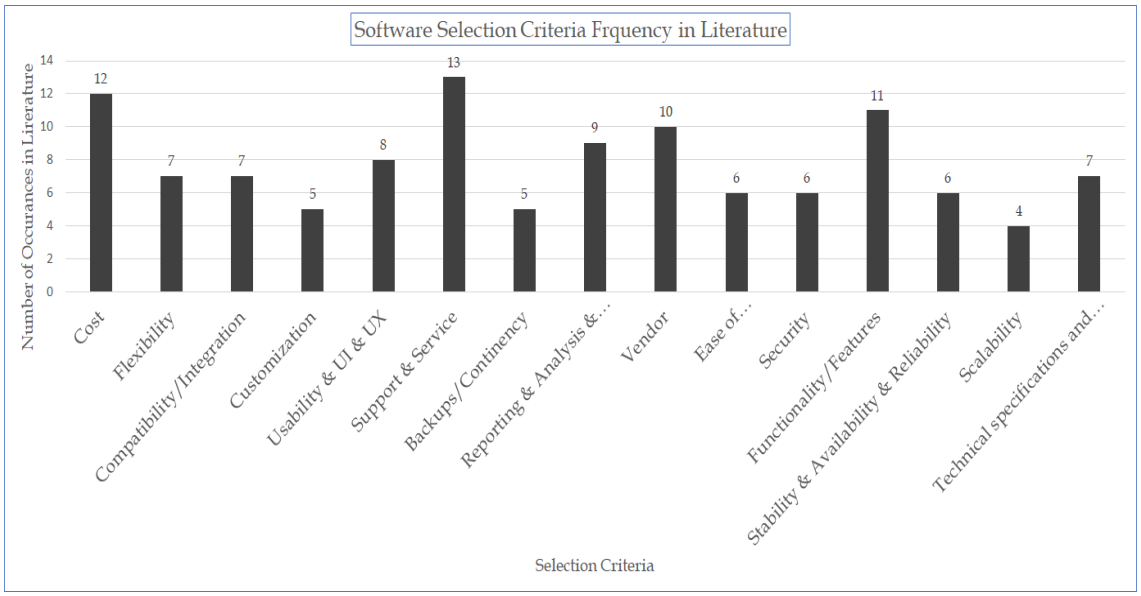

FIGURE 2 Software Selection Criteria Frequency in Literature

Judging by this set of software selection criteria found in relevant academic literature and studies some generalizations about the process and criteria for software selection can be made. As a no surprise, the factor of cost is high up on the list; this could be due to the fact that software is being purchased and outsourced from outside of the organization in the first place to achieve some cost saving measures when compared to developing or maintaining a service within the organization.

The most commonly found selection criteria for software within relevant literature was found to be "support and service" related features. This criterion refers to different types of services that the product vendor offers in combination or in addition with the software that they offer. This result seems rather surprising; surely support services are important but the fact that IT decision makers value support services on par or even more important than the product cost is a significant finding. It could be even generalized that managers and decision makers are so concerned about the performance of the purchased product, that they do not mind the extra cost involved as long as the product is effective and operational with minimal downtime.

Rest of the results did not present any surprising results. Some of the more common selection criteria were as mentioned earlier vendor, functionality & features, reporting, & analysis, and usability. All of these seem fairly normal requirements and criteria for selection for any given organizational software. The importance of these criteria is however changed depending on the purchasing organization, their needs and preferences, and the vision of the decision-making persons within the organization. List of the literature used for this limited examination can be found below in Table 2.

TABLE 2 List of research articles used in examination of software selection criteria

Research article	**Number of Selection Criteria**
Alanbay, (2005)	11
Lang, Wiesche & Krcmar, (2016).	12
Lin & Wang, (2011).	5
Sahay & Gupta, (2003).	8
Marr & Neely, (2003)	8
Benlian & Hess, (2011).	7
Repschlaeger, Wind, Zarnekow & Turowski, (2012)	17
Arditi & Singh, (1991).	5
Lai, Trueblood & Wong, (1999)	4
Ngai & Chan, (2005)	12
Jadhav & Sonar, (2009)	9
Keil & Tiwana, (2006)	7
Clemons & Chen, (2011)	5
Tam & Tummala, (2001)	11
Davis & Williams, (1994)	10

When the generic AHP model for software selection, that was introduced earlier during this thesis, is combined with the software selection criteria found in relevant literature, one can present a highly generalized software selection model that is based on the AHP model. The basic principle is that taking the most commonly appearing software selection criteria and applying them into the AHP model, we are presented with a highly generic model for selecting appropriate software.

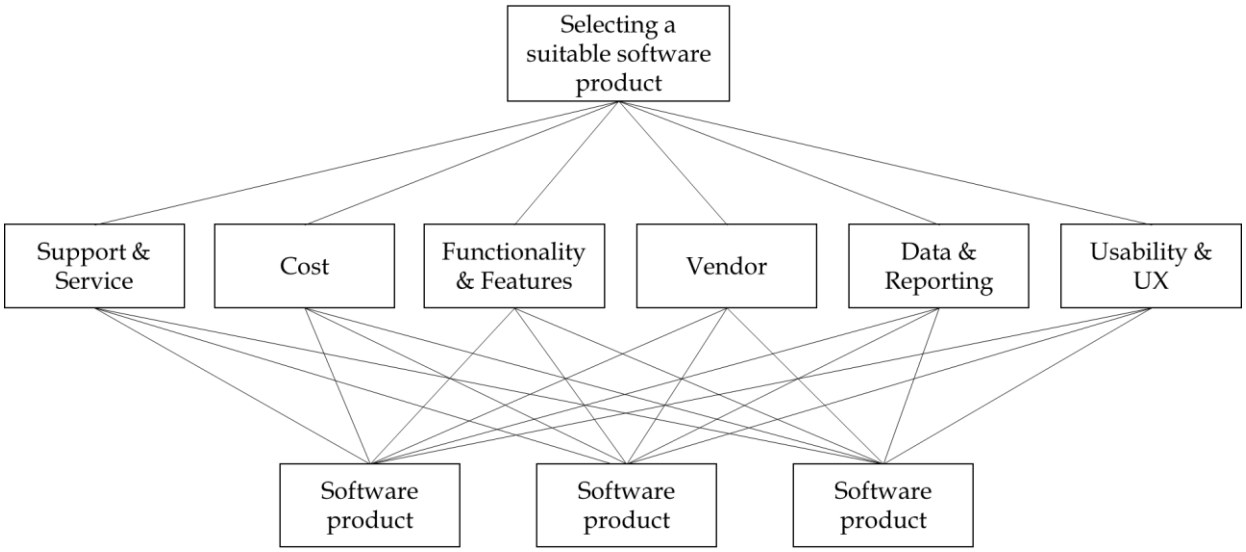

FIGURE 3 Generic adaptation of the AHP model with most common software selection criteria.

4 THEORETICAL FRAMEWORK

The previous chapter has introduced and elaborated on the topics of software selection and password manager selection in organizations. This chapter will summarize these findings in the form of theories relating to these previously studied topics.

4.1 Software selection process

Various findings regarding the process of software selection have been introduced earlier in the literature review of this thesis. This chapter will present theories that have been derived from these materials. The theory will serve as a basis for the formulation of the empirical research that will be used to examine these topics.

One reoccurring theme in literature regarding IT procurement processes and software selection from third party vendors is the fact that the process is interdisciplinary and requires the efforts and input from several parts of the procuring organization in addition to merely the IT department and its subject matter experts. (Heckman, 2003; Lai et al., 1999). Based on the literature review it can also be concluded that the process of selecting software products as an organization is heavily situation and context dependent. Thus, the process of determining what criteria have importance regarding the selection of one type of software can yield entirely different outcomes for another type of software product, meaning different types of products seem to require a different set of selection criteria with differing weights placed on each criterion. (Benlian & Hess, 2011.)

Several studies regarding software selection and its methods also present their own set of selection criteria that they deem important in the process of selecting appropriate software products, a list of these studies can be found in Table 2 on page 27. Some research papers attempt to formulate their own list universally important or generic list of software selection criteria as well

(Jadhav & Sonar, 2009). These types of studies have already been summarized earlier in the chapter 2.3.5. These factors implicate that generic software selection criteria can be defined to be used in software selection processes in organizations. This theory will be tested during the empirical research process of this thesis.

Many different types of models are also introduced in research papers that attempt to conceptualize the process in which organizations select software products and how organizations determine which product is the right one for them. One of the most mentioned models used in assessing and selecting software products was the AHP model or a version of it (Alanbay, 2005; Lai et al., 1999; Ngai, & Chan, 2005; Jadhav & Sonar, 2009; Tam, & Tummala, 2001; Mamaghani, 2002). It became apparent during the literature review that some organizations that use some type of a model to assist them in their selection process did not place any weighs on criteria that were used to assess the products, meaning that the criteria that mattered more were as significant as criteria that were not as important (Benlian & Hess, 2011). Software selection models and their utilization will be examined during the empirical research process to shed more light onto this topic and to support the rest of the thesis.

In summary it can be stated that the academic literature regarding software selection and IT procurement processes is somewhat scattered and lacks coherency. Many academic papers and studies develop their own new models that aim to explain the process of software selection and evaluation, while others focus on examining how the selection process works in certain specific contexts. Other than some individual studies, no common or generic software selection methods seem to exist. The empirical research of this thesis will delve into this topic to find out whether or not the findings of the literature review are also present in the results of the empirical research.

During the literature review it became apparent that certain software selection and evaluation criteria keep resurfacing across different academic studies. It should be studied during the empirical research process if these same criteria are also present in the results of the empirical research process of this thesis. The frequency of these criteria and their importance should also be studied and compared to the findings of the literature review.

To study these theoretical findings of the literature review, the following research question has been formulated: Can generic software selection criteria be defined? The purpose of this question is to examine the relationship of the introduced theory and the results of the literature review.

4.2 Password manager software

As stated earlier in this thesis, password managers are software products that can be used by organizations or individuals to improve their security and password practices. A basic theory on the important facets of password manag-

ers can be formulated based on the findings of the literature review. This theory will guide the empirical research of this thesis and its design.

The importance of usability in the context of password managers arises repeatedly in literature (Karole et al., 2010, Aurigemma et al., 2017; Fagan et al., 2017, Chiasson et al., 2006). As numerous different research papers have noted that the usability of password managers is paramount in order for the product to achieve a high degree of utilization amongst a user groups, it is fair to theorize that usability should likely be an important criterion when it comes to the selection of those types of software products.

Users' doubtfulness of password manager software, its benefits, and the general security of password manager products are mentioned in research papers numerous times (Chiasson et al., 2006; Fagan et al., 2017; Karole et al., 2010). Based on this information, organizations that prioritize convincing users of the products usefulness and selecting a product that suppresses the doubts that users generally have towards password manager products should be a top priority for organizations evaluating and selecting new password manager software. Additionally, the frequent mentions of both legitimate and unfounded security concerns regarding password manager products and their usage should be noted by organizations while selecting between competing products (McCarney et al., 2012; Gasti & Rasmussen, 2012; Silver et al., 2014; Zhao et al., 2013).

Based on these aforementioned theoretical findings a research question can be formulated: What are the most important criteria when selecting a password manager software product? The purpose of this question is to find out if the views of organizations and IT professionals differ with the information that can be found in academic research articles and if industry practitioners are aware of these issues that surfaced from academic studies. Additionally, the following research question will be answered in order to study the relationship and differences of the selection processes of password managers and software products in general: Do the selection criteria for password managers significantly differ from selection criteria of software products in general?

4.3 Summary of theory

The purpose of this chapter has been to introduce theories relating to the topics of this thesis that the empirical research portion of this thesis will attempt to examine in detail. Purpose of the theory is to propose questions and assumptions based on the material and information that has been derived from the literature review which will be then examined through the results of the empirical research process. The results of the literature review presented in the previous chapters will guide the design and formulation of the empirical research.

The previous chapters elaborate on the topics of this thesis in great detail. The previous chapters also lay out what existing research knows about the topics and concepts of this thesis. Based on the information extracted from the aca-

demic papers an empirical research can be created. The purpose of the empirical research process it to evaluate and examine how and if the conclusions and findings this thesis can also be observed in an empirical study context.

The purpose of studying the process of software product selection was to lay out a foundation on which the selection process of password managers can be examined. Without creating a baseline of knowledge on how software products are selected in general, it would be difficult to understand the process where password manager products are selected. Once a good understanding of how software selection processes are carried out and a theoretical understanding of the process is achieved, one can apply this knowledge to evaluate the process of selecting password managers and the potential differences in the selection process between different types of software products. In summary it can be stated that based on the results of the literature review the research regarding software selection methods is scattered and really no consensus can be found between the academic papers and studies regarding the topic. Some specific selection criteria that are used to evaluate the competing software products do however resurface many times in the material that was covered by this literature review. These resurfacing criteria can be used to form a theory on which selection criteria are important when selecting software products. This theory will be tested during the empirical research process to see if the theory and findings hold any ground in an empirical context. Additionally, it became apparent during the literature review that no common or universal methods and defined frameworks to assist individuals and organizations on the process of selecting software products really exist. This theory will also be tested during the empirical research process to see if it is so that neither academic research papers and industry practitioners do not utilize any established software selection models or frameworks.

Password managers and their selection processes are the main focus and interest of this study. Password managers have been extensively studied from multitude of viewpoints and contexts of which many are covered in the literature review portion of this thesis. Across these studies certain trends and concepts emerge repeatedly which can be used to form a basic theory on which factors are important when trying to evaluate these types of products. This theory will be tested during the empirical research process to see both if industry professionals recognize the same criteria and aspects of these products to be important and if the theory of the academic research is aligned with the findings of this empirical research. The results of the empirical research regarding password managers will also be compared to the findings relating to the general process of software selection to determine if the selection process of password managers and their selection criteria are significantly different from each other's.

This concludes the portion of the thesis in which a literature review has been conducted and theory has been extracted in order to gain sufficient information regarding the topics of this thesis and to be able to formulate an effective empirical research process and design. The following chapters will detail the empirical research process and its design.

5 EMPIRICAL RESEARCH DESIGN

5.1 Research objective

The purpose of this thesis is to find out the most significant and deciding factors of why organizations choose one password manager software over another. In addition to this the thesis also analyses and discusses the topic of software selection in organizations in general. Earlier in this study I have presented my findings of generic software selection criteria and which criteria is used most frequently. By combining the findings of this thesis with the empirical research presented later we will be able to answer the research questions posed in this thesis as well as gather meaningful insight on what factors and criteria drive the selection of certain password managers.

As stated earlier, the purpose of this thesis is to determine the reasons of why an organization chooses one password manager over others that are available in the market. The ultimate goal is to be able to answer the main research question of this thesis:

- What are the most important criteria when selecting a password manager software product?

This main research question will be supported by the following additional supporting research questions:

- Do the selection criteria for password managers significantly differ from selection criteria of software products in general?
- Can generic software selection criteria be defined?

By answering these abovementioned questions, this thesis will be able to shed some light into the selection process of password manager software and what factors drive industry experts to choose one product over the other. Meaningful

comparisons between the selection criteria and motivations of password managers and software in general can be derived from the research results.

5.2 Research design & method

The empirical research of this thesis was conducted as a qualitative single case study. Qualitative methods are used due to the topic of this master's thesis being qualitative. Single case study is appropriate for this particular research process as it can produce highly detailed information regarding a specific topic (Eisenhardt & Graebner, 2007). Utilization of the case study method is also appropriate as the goal of this study was to gather empirical data on the selection process of password managers in a real-life setting (Benbasat, Goldstein & Mead, 1987). Case study research is also suitable for studying the phenomenon of this article due to the fact that it is suitable to be used when studying concepts related to information systems and the relation of information systems to organizations that utilize them (Darke, Shanks & Broadbent, 1998; Benbasat et al., 1987).

The selected method of gathering empirical data were structured interviews. Structured interviews were selected due to the nature of the needed data being qualitative and the fact that the purpose of the interviews was to extract in-depth data on a specific topic (Eisenhardt & Graebner, 2007). By using structured interviews, it was possible to gather in-depth comparable data while giving the interviewees an option to freely express their own views on the subject. The interviewees' ability to express their opinion and expertise on the subject matter was determined to be the best way to extract the needed information in order to answer the research questions of the thesis, as the practical expertise and knowledge of the interviewees was required to achieve that. (Darke et al., 1998.)

The topic of the thesis and the empirical research process was specific and technical in nature which meant that the interviewees from which the data would be gathered from should adhere to certain requirements in order for them to be valid participants. In order for an interviewee to be qualified for the interview they needed to possess sufficient experience and knowledge on the core subjects of this thesis. Thus, it was determined that the participants should be knowledgeable and experienced at the very least in the field of information technology and that they should have actively participated in the selection of software products within organizations. By narrowing down the possible list of eligible participants with these limitations it was possible to gather relevant and precise empirical data on the topics that this thesis is attempting to study. If the participants would have limited knowledge and experience on the selection of software products their input would not be relevant to the purposes of this empirical research and thesis.

5.3 Research analysis

The interviews were conducted remotely during the months of January and February in 2021 using video conferencing tool Microsoft Teams. The interviews were conducted remotely due to the at the time ongoing coronavirus pandemic. All the interviews were conducted in Finnish. The interviews were recorded for later stage analysis and notes were taken both during and immediately after each interview. Average duration of a single interview was 21 minutes and 14 seconds across 12 interviews. Total of 12 participants took part as interviewees of this empirical research. All of the interviewees met the predefined criteria of having experience in the process of software selection in organizations. The interviewees included subject matter experts, technical specialists, and managers in deciding roles within their organization. The average IT industry experience of the interviewees was 21,08 years.

The results of the interview process were analyzed by utilizing thematic analysis methods. Purpose of thematic analysis is to provide a method to analyze qualitative data in a systematic and a reliable way to provide meaningful and accurate analysis on the raw data in question (Clarke & Braun, 2017; Nowell et al., 2017). Initially after the interviews were completed, the data was fully written out for each interview. This raw data was all analyzed, and the most significant and relevant results were first marked and then transferred to another space for further analysis. Once the more significant and meaningful data had been extracted from the unfiltered interview results and moved, it was analyzed once again and refined even further by coding the data based on what certain concept it was regarding and which research topic it fell under. After this some clear concepts, themes, and conclusions could be made out from the data. These emerging concepts were grouped together based on the topic they covered in order to form coherent conclusions and to tie them together with other concepts present in both interviews and previous research. Finally, the refined results were included in the study itself to be further examined and discussed upon. The analysis of the data was carried out by using mostly the combination of Microsoft OneNote to process data in text form and Microsoft Excel to process the results in a table form and to create descriptive charts to illustrate the findings in a meaningful way.

During the interviews, the same interview structure and questions were used for all participants. The interview structure can be found in Appendix 1 in the end of this paper. Only some additional questions were asked from the participants if the interviewer felt that their answer needed additional clarification or if the interviewer felt that additional useful data could be extracted by asking an additional question relating to a single topic. The interview structure that was used was comprised of two main sections. The first section included questions relating to the process of software selection within organizations and the selection criteria of software products. The second section of the interview included questions regarding password manager products and their selection

process, selection criteria and general beliefs and attitudes towards their usage. The two main sections were constructed in parallel so that the answers of the different sections could be meaningfully and easily compared. Afterwards the results of the empirical research process were examined and analyzed. The following chapter will introduce the results of the empirical research process.

6 EMPIRICAL RESEARCH RESULTS

6.1 Software selection in organizations

The first major section of the interviews was an attempt to gather insights and knowledge on how organizations and professionals assess software and how the decisions to acquire a single product are made. The interview participants were asked to consider any recent or major processes or projects in which they have been a part on that resulted in some software being selected to be used within the organization they represent. The way the questions were setup was purposefully open ended in order to encourage the interviewees to express their general feelings on what they consider to be important in the process of software selection.

Two of the most prevailing themes across the board in the interviews were cost of the software and the ability of the software to fulfill business needs. Many of the participants considered business needs as one of the most important aspects when it comes to selecting and assessing software. The need to fulfill and answer business needs with the software that is about to be acquired was found to be an important aspect and a definite goal of the software selection process, as some interviewees stated that the purpose of the software is to serve some business need. One general trend that could be noticed from the interview results was the fact that people in managerial positions seemed to be slightly more focused on the business purpose and outcome of the selection process, rather than the successful technical implementation of the product that some interviewees in more technical or operations positions inclined to say.

As stated previously cost was one of the two most mentioned criteria the interviewees listed during the interviews. While cost by itself may seem like an obvious criterion at a first glance, many of the interviewees felt the need to elaborate on how cost is important and how it related to other criteria mentioned. It was stated several times during the interview process that while cost is inherently important criteria, it is rarely the one and only deciding factor

when making a choice on software products. As one interviewee put it when elaborating on the significance of cost during the selection process:

> "…as when it comes to price, [it is important] that it is in line with other equivalent products... …price is in that case perhaps secondary but in a way that it is somewhat in line [with other products]."

It could be summarized that cost was in fact often mentioned as a secondary criterion to some other criteria that was deemed more significant, meaning that price and cost do matter but ultimately other criteria and perspectives can turn out to be more influential while making the final choice.

Beyond fulfilling business needs and cost of the product, most other criteria were only mentioned few times or just once. These less frequently mentioned criteria that were mentioned multiple times included usability of the software, support and service offerings, and the vendor and their behavior. However, no universal generalizations can be made beyond what has already been mentioned about business needs and cost of the products regarding the importance of selection criteria.

Respondents that were concerned about the usability of the software expressed their concern over the fact that if the software product that was going to be selected was too complicated to use it would incur additional charges due to the end users of the software not being able to use it properly or not being able to utilize the software to its fullest extent. One interviewee stated the following regarding the significance of easy usability for end users when asked to elaborate on what factors are important when choosing between different software products:

> "How much effort does the product need in order for it to be usable… …If you have even a little bit cheaper product but launching it is difficult and it is hard to understand them maybe it is sensible to pay a little bit more, because in the long run you will save money."

Therefore, it could be said that in some cases if one software product is more usable and easier for users to learn, a higher initial price of the selected software can be justified over a competing cheaper software product that is harder to use and will thus incur costs via additional training and wasted resources.

Support and service offerings refer to support services that the software vendor offers alongside with the core product or solution that they are selling to customers. It could be generalized that individuals that worked in operational or technical roles were more concerned over the vendors support service offering and its quality. One respondent went so far as to say that the software products support services was one of the key aspects of why one specific software product was chosen over another in one particular selection process.

Vendor of the software product was deemed to be an important factor when choosing between competing products as well. However, different interviewees saw the significance of the vendor from rather different perspectives. In general, the interviewees that mentioned the vendor as a meaningful factor

in the selection process of software products felt that the vendor should be involved in the process and for it to provide some assistance over the course of the selection process. Also, the trustworthiness, reputation, and the image of the vendor was mentioned as a factor. The behavior of the potential vendor or their representatives was also mentioned in a negative fashion over the course of the interviews; a negative experience with a single vendor can cause them to be rejected even though there might have not been anything inherently wrong with their product. This negative experience could be anything from delayed response times to experienced bad service in general.

The interviewees were also challenged to provide three "universally important" selection criteria that are important defining criteria when selecting almost any type of software. In general, the interviewees felt that this particular question is challenging or even impossible to answer, because the interviewees felt that important selection criteria depend too much on the type of software being chosen as well as the particular environment and context it is supposed to be selected to. However, the interviewees were able to provide answers to this purposefully challenging question that yielded some interesting insight.

The single most mentioned criterion was price, which was listed as one of the three most important selection criteria by eight interviewees. Even though this is not surprising per say, it interesting that even though participants earlier indicated that price is rarely the deciding or most important factor it was still easily the single most mentioned criterion with 2/3rds of the interviewees mentioning it.

Rest of the answers to this question were however more scattered. Answers relating to usability, support services, suitability, and the actions of the vendor all received three votes each. Rest of the criteria mentioned as an answer to the question posed received two or one votes, out of which no recognizable pattern or trend could be derived. In total the 12 participants gave out 18 different unique criteria when asked to list the three most important software selection criteria.

Lastly as a part of this section the interviewees were asked to simply give a number grade estimate between one and five on how important they consider a single given criterion to be. One meaning that the particular criterion is meaningless or irrelevant most of the time when assessing software, and five meaning that the specified criterion is important in almost every single software selection process or project. The list of 14 separate criteria that the interviewees had to assess is the exact same as the list of criteria mentioned on page 26 and figure 2 of this thesis, except with the criterion of "Reporting & Analysis & Monitoring & Data" being left out. Some of the interviewees also thought that assessing software selection criteria like this without any context is challenging and some individual criteria had to be skipped. However, this exercise provided some rather interesting quantitative data to compliment the otherwise qualitative nature of this thesis and empirical research.

The following Figure 4 presents the results of this criteria assessment exercise. Some clearly distinguishable trends that emerged from this dataset can be

noticed right away; the criteria of security, stability & availability & reliability, features & functionality, backups & contingency, usability, and compatibility/integration were the only criteria to score an average of over four points. While some of these criteria were mentioned during the rest of the interview as well, the importance of security is highlighted in any capacity for the first time. Security was not mentioned more than a few times by only some individual interviewees during the previous questions that were posed to them. Compatibility and integration were also highlighted as an important criterion for the first time during this particular exercise. Rest of the criteria scored somewhere between 3 and 4 without any mentionable trend present. Interestingly cost only scored an average score of 3.5 during this assessment. Previously highlighted criteria of vendor also scored comparatively low with the average score of 3.3.

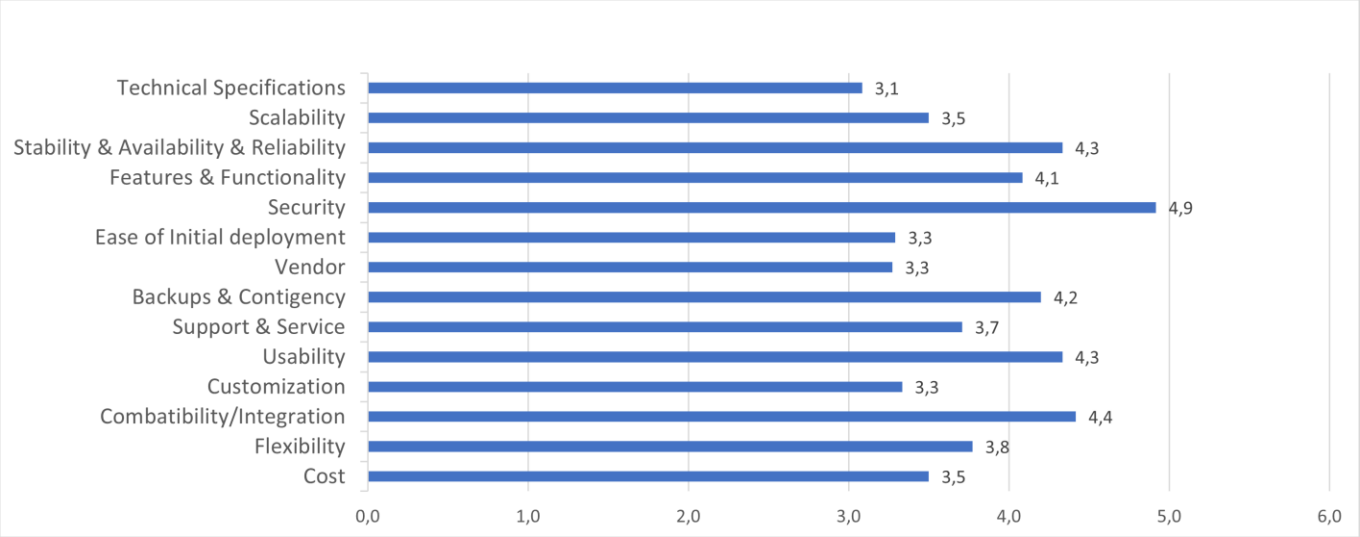

FIGURE 4 Software selection criteria assessment

6.2 Utilization of models and theories in software selection

As a part of the interview the interviewees were asked to elaborate on their past usage of models and theories as parts of software selection processes, and the usefulness of them. Out of all the interviewees half said that they used some type of a model as a part of the software selection process while half said that they did not utilize any models. Out of all the interviewees that answered that they did use some type of a model as an aid in the selection process none referenced any established or predetermined models and frameworks. The participants instead elaborated that they used basic comparison methods by listing requirements and then comparing the products. Testing and proof-of-concept processes were also mentioned as an important aspect of comparing the candidate products. The respondents who said they had used some type of a selection model to assess the competing products said that the usage of those models was useful and beneficial in coming up with the final selection. One interviewee stated regarding the usage of models during the selection process:

> "Absolutely… …when you ran the results through it [the model assisting the selection] we started to see differences right away…"

All in all, no clear consensus or trends could be spotted from the empirical research results regarding the past usage of software selection models and theories. The models that the interviewees stated they had used were different between one another and often had been built from scratch by themselves. The results of this empirical research seem to support the notion also spotted in studies and in the theoretical section of this thesis, software selection processes and practices tend to vary quite a lot depending on who you ask, and no clear established methods or frameworks exist.

When the interviewees were asked whether or not some type of a universal or predefined and preset software selection model or a framework would be useful in their future software selection process efforts, all interviewees responded positively. Interviewees in general saw real value in some type of commonly accepted model or a framework that would assist in the selection of software products.

However, after the interviewees had given a positive answer, they almost universally and immediately noted that they do not know whether or not creating a viable, usable, and helpful preset and predefined model is even possible. Interviewees were concerned that if such a model would be created that it would not be universally functional as different types of software for different needs should be evaluated differently. Therefore, it seems that some type of a general model that assists in the selection process of software products would be welcomed, but widespread doubt about the functionality and feasibility about the successfulness of such a model are present based on the results of this research process.

6.3 Password manager selection in organizations

The last major section of the empirical interviews delved into the topic of password managers and their selection processes in an attempt to gather empirical real-world data on how organizations and industry experts see and select these products. While all participants were familiar with the concept of password manager software and were able to give an expert opinion on the matter, six of the total 12 participants had been personally involved in a process or project in which a password manager product was selected for an organization.

Initially as a part of this section on password manager selection the interviewees were asked to give their opinion on what factors or features they consider to be generally important from an organizational standpoint regarding the usage of password manager products. Commonly resurfaced themes included usability, security, and the products support of multiple platforms.

Usability was by far the most mentioned single factor when the interviewees were asked to describe what they consider important relating to the usage

of password manager software within organizations. Eight interviewees out of 12 total mentioned usability as a significant factor relating to password manager software in organizations. Usability in this case includes several different meanings and viewpoints. Usability from both the end user as well as the system administration point of view were found to be important. While the importance of usability from an end user standpoint was recognized by several respondents, the usability and ease of use from an administrative standpoint was found at times to be one of the deciding factors between competing products. The general consensus regarding usability can be summarized as "it just needs to work". There seems to be very little patience for password managers that are difficult to use in comparison to other competing products and the importance of easy usability from end user perspective is often understood.

Security was the second most explicitly mentioned single factor or feature that the interviewees mentioned as an important aspect of password manager software. Total of six interviewees out of 12 mentioned security as one of their top concerns. Even though every interviewee seemed to agree on the importance of security some individuals elaborated on why they thought that criterion was especially important in the context of password managers. One interviewee stated relating to the security and the integrity of the product that:

> "The reliability and trust of the product are key factors because people are inputting secrets, and the trust cannot be gained back if it is lost."

Another interviewee elaborated that password manager products can be viewed as safes, which is why security and integrity of the product are one of the most important criteria while selecting such a product. Therefore, it can be summarized that the security and it's importance is clearly recognized by subject matter experts.

The third most mentioned single factor was the multi-platform support of the password manager product. Multi-platform support in this context refers to the products ability to provide the software in different types of devices and environments, instead of it being usable only on one platform such as a desktop computer. The interviewees felt that it is important for the password manager software to be able to adapt to all sorts of devices and environments, due to the fact that if the software would not be able to support some common platforms it would heavily degrade the usability of the service and thus not provide the sought-after benefits password managers are supposed to deliver. This requirement of multi-platform capabilities ties in closely with the earlier mentioned criterion of usability of the product.

The remaining factors and features that the interviewees considered to be important in relation to password manager software included features, vendor and its characteristics, reputation and trustworthiness of the product and vendor, availability of the software, among other less mentioned factors.

The interviewees were also asked to rate specific software selection criteria relating to password managers on a scale from 1 to 5. The list of criteria that the interviewees were asked to assess was identical to the list of criteria mentioned

in the earlier section 5.1. Purpose of this exercise was to see whether or not the interviewees felt that different criteria were more important or less important in the context of selecting password manager products when compared to software in general.

The results of this exercise can be found in Figure 5 below this section. In general, it can be concluded that no significant differences were found based on this graph and its data alone. Out of the 14 total criteria, based on which password manager software can be evaluated on, the interviewees found the following six to the most important and only ones to score an average rating of over 4: stability & availability & reliability, features & functionality, security, backups & contingency, usability, and compatibility & integration. Out of these criteria, security was the only single criteria to score an average of five points, meaning that every interviewee rated the importance of this criteria extremely high. Otherwise, all of the six criteria to score the average score of above four points were the exact same criteria that scored an average score of above four points in the comparable exercise in the context of general software selection as mentioned earlier in this chapter. All in all, the results of this exercise did not provide any significant differences between the interviewees appreciation of generic software selection criteria and the same selection criteria in the context of password manager software.

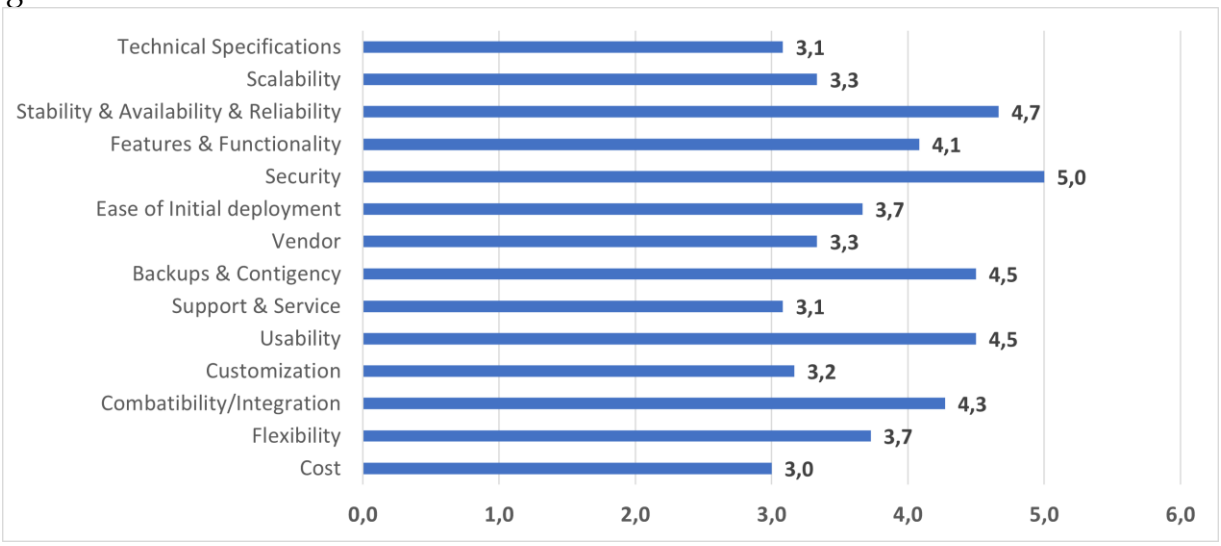

FIGURE 5 Password manager selection criteria assessment

The most significant portion of the password manager related question set was however the interview questions relating to the empirical experiences of the interviewees relating to real-world processes in which they have selected password manager products to be used in organizations. As mentioned previously, six out of the 12 interviewees had participated in the selection of a password manager product at least once. The interviewees represented individuals in both managerial as well as more technical positions. Some participants had participated in the selection of a password manager several times. The interviewees were asked to freely elaborate on the password manager selection pro-

cess they had been involved in and to share their experiences on the details of the process and its outcome.

Overall, much like the findings of the earlier section of this empirical research regarding general software selection practices and processes, so far the empirical findings relating to password manager product selection within organizations could be referred to as somewhat scattered. Even though some individual themes and concepts were mentioned by several participants, it is difficult to locate any sort of overarching theme or universal narrative on password manager selection beyond a couple of individual themes and concepts. Even though some particular criteria were mentioned by many interviewees, the same concepts were not mentioned at all by some. It could be summarized that in general the organizational role of the interviewee reflected on the aspects of the password manager that they personally thought were important when also selecting the product. Some individual concepts and important commentary were however discovered during this empirical research process which will be introduced next.

Price was once again a reoccurring topic of discussion in this part of the empirical research process as well. Four out of six interviewees mentioned price as a deciding factor when making the selection of a password manager product. Price was not however mentioned as a single or a decisive criterion when it came to the final selection. Price was seen as merely just another criteria among several others. Some interviewees elaborated on the importance of price regarding the selection of password managers and said that while price matters it is not a determining factor in the final decision.

In general, the functionality and other criteria were deemed to overrule price in importance. As to why price is not considered to be important factor in this specific context, one interviewees answer summarizes the concepts quite bluntly:

> "Of course, the price matters as well, but when we are talking about password manager systems, they are usually quite cheap… …but of course price had a role when the selection was made."

Password managers can indeed be characterized as simple products, especially when compared to more complex products that have multiple use cases and dependencies. Even though this signals that sometimes organizations might not care as much about the final cost of the product as much due to its cheap price in the context of enterprise software, it means that the actual product and its functionalities need to be clearly superior to the competing products. As another interviewee put it:

> "The features of the product were pretty close to each other so it came down to the pricing… …the other product would have required much more setting up and would have been much more expensive because of that."

as the functionalities of the competing products were highly alike, price turned out to be the deciding factor in that specific selection process.

Another concept and criteria to repeatedly resurface during the interviews was compatibility. Compatibility in this context refers to how the password manager product is compatible and integrates with the existing IT infrastructure and environment. Five out of the six interviewees to have participated in the selection of password manager products listed some variation of this criterion when they were interviewed. However, the interviewees notions on why the compatibility and capability to integrate to the organizations existing infrastructure differed slightly depending on if the interviewee was in a managerial or in more of a technical role.

Interviewees in more technical roles indeed considered integration and compatibility with current infrastructure as an important criterion when it came to making the final selection on the password manager product. If the product is able to support these requirements it easier and faster to take into use within the organization. One interviewee noted that it was noticed during the password manager selection process that competing password manager products had clearly different levels of possible integration and compatibility within their existing IT infrastructure and environment. This clear difference in compatibility was listed as one of the main criteria that led to the final selection of the chosen product. In general integration into other supporting systems such as access management solutions or the ability later expand the usage of the product were deemed to be important as well.

Interviewees in managerial roles also considered compatibility and integrability of the product as important factors. Interviewees in managerial positions tended to give more consideration to the overall implementation compatibility of the password manager, meaning how the product suits the organization and its workflows and processes, instead of how the product suits the organization and its processes in a technological sense. Even though interviewees in managerial positions gave consideration to the overall implementation and the organizational value that the product brings, they also considered the technological integration to be an important aspect in the selection process.

The interviewees were also asked if they felt that the password manager selection process they participated in was ultimately successful. All six interviewees to have participated in the selection of at least one password manager product answered that the selection was successful, and that the product meets expectations. This result can be interpreted to mean that the selection criteria and methods described by the interviewees displayed at least some real-life credibility, even though this success was self-reported.

6.4 Empirical research results summary

This chapter will summarize the results of the empirical research and highlight the most significant findings of the empirical research process. The implications

of these results and their relationship with the results of the literature review will be elaborated on the following discussion chapter.

The empirical research results regarding the software selection processes in organizations can be summarized as follows. The importance of business needs and price of the product is highlighted across the interviews and can be thus considered to be rather significant criteria across all software selection processes regardless of what type of software is being acquired or evaluated. The security of a software product was recognized as important when explicitly asked about but was not mentioned by the interviewees unprompted. The significance of some selection criteria fluctuates depending on the organizational role of the individual conducting the selection or evaluation of a software product. The importance of several individual criteria is highlighted in cases where the products being compared are similar enough in the more important aspects such as price and ability to fulfill business needs. Despite these findings, the interviewees had difficulties in defining any types of universal rules or thoughts regarding the selection of different types of software products.

The interviewees were also questioned on the usage of software selection models and theories and their usage. The results of this were mixed since some interviewees had used them while some had not. No interviewee had used any sort of a standardized or an established model to aid them in the process of selecting software products. Those interviewees that reported they had used some models also stated that the models had been created by themselves. Those that stated that they had utilized models in their selection processes also said that the models were overall useful in making the final decision on the products that were evaluated. In summary, some interesting individual notions and concepts emerged regarding this topic even though it seems no elaborate conclusions can be drawn from these results.

Findings regarding password managers and their selection processes are the following. It was established during the interviews that usability and security are two of the most important criteria when selecting and evaluating password manager products. Price was determined to clearly remain as a secondary criterion to other more significant criteria when evaluating and selecting password manager products. Beyond these findings it is hard to find any other clear trends regarding individual selection criteria among the interview results. Similar to the earlier section relating to software selection processes in general, how individuals value certain criteria seems to depend on their organizational role and position.

One section of the empirical research was an exercise in which the interviewees were asked to rate the importance of specific criteria that can be used to evaluate software products on a scale from one to five. The same criteria and question formation were used for both evaluating software products in general as well as evaluating password manager products. This allows for the comparison of how the interviewees graded the importance of specific criteria in the context of software in general compared to password manager products. Following Figure 6 presents the results of this exercise in a figure format:

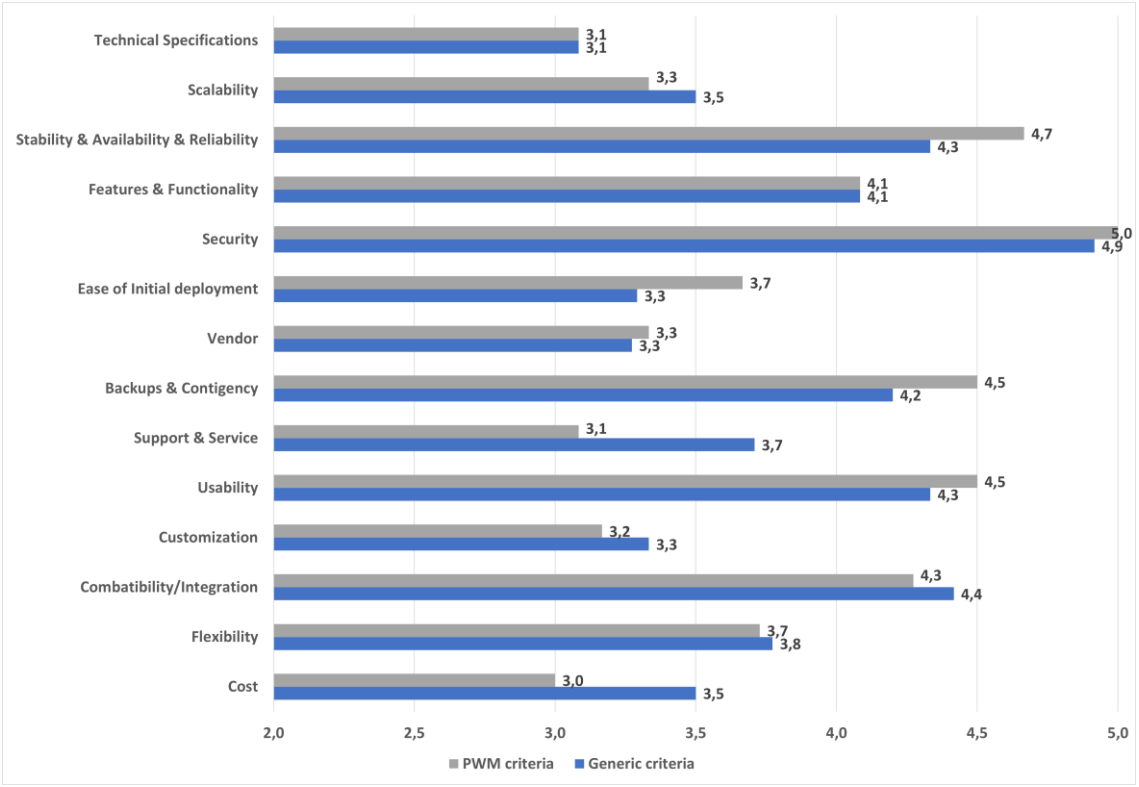

FIGURE 6 Password manager and generic software selection criteria compared

By analyzing the Figure 6 we can conclude that the interviewees rated the importance of these criteria in a fairly similar fashion regarding both password manager selection criteria and software selection criteria in general. Most of the listed criteria were rated more or less similarly. Some criteria were rated differently however, cost and support & service criteria both had rating difference of 0.5 or more between the contexts of selecting password managers and generic software. This implicates that support & service features and the price of the product could be more significant when evaluating password manager products when compared to software products in general. Other differences were smaller and considering the sample size no conclusions can be made based on these differences.

7 DISCUSSION

The following section will discuss and analyze the results of the empirical research and its relation to the literature review's findings. Additionally, the research questions of this thesis will be answered.

7.1 Software selection process findings

One of the most prevailing themes across the interviews regarding software selection methods was the acknowledgement that cost and business needs are the primary drivers of why software products are chosen. However, even though the significance of price was clearly mentioned during the interviews, the overall significance of the price fluctuated significantly and depended on other factors and criteria that were deemed more important in those particular selection processes. The significance of price is highlighted in both academical texts on the subject of software selection as well the empirical research (Lin & Wang, 2011; Keil & Tiwana, 2006).

Another standout criterion when it came to software selection criteria was the software vendor. The significance of the vendor was elaborated on several times, and especially the reputation or the quality of their service and communications was a notable factor while choosing an appropriate software to purchase. This criterion did not however play as significant role in the selection of password managers, even though it was mentioned during the interviews. This finding seems to also support the frequent reoccurrence and the importance of the vendor in academic papers relating to software selection methods (Ngai & Chan, 2005; Jadhav & Sonar, 2009; Clemons & Chen, 2011).

The interviewees indicated during the interviews that they would be open and interested to utilize a standardized and preset framework or a model that guides the selection process of software products. The interviewees did however display doubt on if creating such a model would even be possible. Whenever the interviewees stated that they had used some models to assist them during

the selection process of some software products they elaborated that the models they used were mostly created internally and by not using any existing models as supporting material. This supports the notion of the academic papers that the models and methods organizations utilize to select software products are scattered and in general the process lacks a formal theory (Badampudi et al., 2016; Heckman, 1999; Keil & Tiwana, 2006; Jadhav & Sonar, 2009). As to why such a model or a framework has not been created, perhaps the notion that was brought up by the interviewees that the creation of such a model would be challenging or even impossible.

7.2 Password manager findings

Researching and analyzing the selection of password manager products was the main focus of this thesis. Some insightful results and conclusions can be made based on the results of the empirical research. The empirical information gathered from the interviews was insightful and meaningful. The data that was gathered is also sufficient to answer the research questions of this thesis later on.

The empirical research and the interviews revealed some meaningful notions on how organizations conduct the selection process of password manager software. Across the interviews it became clear that the personnel that are involved in assessing these products and making the ultimate decision on what product the organization will acquire will favor the criteria of the software that are the most relevant to them in their own position within the organization. Meaning that those involved in more technical or operational roles seem to prefer a product that will suit them the most in their daily work. Meanwhile persons in managerial positions seem to have the greater interest of the organization and the purpose that the product is supposed to fulfill in mind. It is important to note while that this trend could be spotted across the interviews and empirical data gathered, it can not be said that operational employees do not care about the organizational impact and implications of the product or that managers are not interested on how the daily administration tasks are conducted as both of these groups did also consider the criteria that was important to the other group during the interviews. These individuals in different roles simply saw these criteria in a different light in relation to their own organizational roles. The implication of this finding is that it is vital for the successful selection of a password manager to include persons from different types of roles and parts of the organization into the software evaluation and selection process in order to account for these biases when making the final selection on a product.

Another significant theme when discussing purchasing something is the cost of the product. Cost and price of the product turn out to be concepts of which importance is difficult and complex to determine when it comes to selecting password manager products as at the same time price does and does not matter. As the interviewees themselves mentioned during the interviews, price

matters when making the final decision. However, other factors and criteria can overwrite the significance of price of the product quite easily as those factors are deemed more important. It also seems to be so that the price of a product is more significant when there are two similar competing products that offer the same value in other aspects such as features or usability. Meaning that if the two competing products are similar in terms of features, functionality, and other aspects that the organization deems important then the significance of the price of the product is increased. In a sense it could be simplified that the price sensitivity of the purchasing organization becomes greater when the competing products on the market are close in terms of the considered criteria and features. This effect works the other way around too; when the products being compared are clearly different in the way of functions and features the price of the product becomes less important due to the fact that the organization wants to select the superior product out of the two even if the superior product is significantly more expensive.

The suitability of the password manager into the existing organization infrastructure was mentioned several times an important factor when making the decision on what product the organization was going to ultimately choose. Throughout the interviews it became clear that password manager is seen as a supporting software serving a single simple task. Due to this password manager applications can be considered within the organization to have a supplementary and complementary role. Password managers are not acquired into an organization to necessarily produce or create anything, they are more so acquired to serve as a tool to support other more important processes and applications and to enhance some organizational requirement such as security. Once this supportive and secondary nature of password managers is understood, it is easy to understand why many interviewees felt that the password manager product that is about to be selected needs to "just work". In short, it seems that password managers can be considered to be simple applications that serve a supporting role within the software and service portfolio of the organization.

7.3 Answering research questions

By having had analyzed the results of both the literature review as well as the results of the empirical research we can answer the research questions of this thesis. First answers will be provided for the two supporting research questions and the main research question of this thesis will be answered last.

One of the supporting research questions was the following:

- Do the selection criteria for password managers significantly differ from the selection criteria of software products in general?

After conducting both a literature review and an empirical research process on this topic it can be said that the selection criteria of password managers and

software products in general do not differ from each other's in a significant manner. In general, it can be said that password managers may have a higher need for usability and security when comparing to other types of software, but these same criteria can be considered as important regarding other types of software as well, and they are not important exclusively for evaluating password managers (Arias-Cabarcos et al., 2016; Repschlaeger et al., 2012; Gasti & Rasmussen, 2012). These findings were present in the results of the empirical research as well. However, the differences are not significant, and these criteria could very well be considered to be important for some other specific types of a software products. Of course, decision makers should evaluate what specific criteria should be weighed more heavily regarding certain types of software products, but the same processes and principles apply when selecting either password manager software or other types of software.

The second supporting research question was the following:

- Can generic software selection criteria be defined?

Generic software selection criteria cannot be reasonably defined. It became apparent during the research process that different types of software products are simply too distinctive in order to be evaluated by using the same criteria, and thus the importance of a single criterion can fluctuate significantly depending on the type of the product being evaluated (Benlian & Hess, 2011). Even though some prior research has attempted to create a generic list of criteria to use when evaluating software product, they are rare, and no consensus or commonly used models seem to exist (Jadhav & Sonar, 2009). Additionally, according to the empirical findings of this thesis industry practitioners appear to think that the selection of software products is highly context dependent and therefore any common list of criteria can not be used when evaluating software products.

This brings us to the main research question of this thesis:

- What are the most important criteria when selecting a password manager software product?

Based on the literature review about the topic of password managers and the empirical research into the subject some conclusions can be made. Both the results of the literature review and empirical research indicate that the usability of password manager software should be a leading selection criterion when evaluating, comparing, and selecting password manager products. Usability in an organizational context assures that the highest number of users actually utilize the product in their daily work. If users feel like the product is hard to use and thus shun it in their daily work, the investment into the product goes to waste as the benefits of using a password manager are not achieved. The importance of usability of password managers is highlighted in previous research, as users tend to value the usability of password manager quite highly (Karole et al., 2010; Stobert & Biddle, 2015; Arias-Cabarcos et al., 2016). This finding was reinforced

during the empirical research, as the interviewees indicated that the usability of the product was a leading selection and evaluation criteria for these types of software products.

General security of the password manager product was brought up in both previous research as well as the empirical research process conducted as a part of this thesis. Security of password managers was found to be important from both organizational and user point of views. It was brought up during the literature review that even though some password manager vendors advertise their product as secure and safe the reality can sometimes be the opposite (McCarney et al., 2012; Gasti & Rasmussen, 2012; Silver et al., 2014; Zhao et al., 2013). This means that organizations wanting to acquire password manager products into their organization need to be aware of these risks and to remain vigilant while evaluating these products. However, as it was discussed during the empirical research process, individuals responsible for the selection of password managers did in fact consider the security of the product to be an important aspect in the final selection of the product. It also became evident during the literature review that users are often concerned about the safety of these products, which means that the organization need to take the security concerns of the users into consideration as well (Chiasson et al., 2006; Fagan et al., 2017; Karole et al., 2010). Therefore, it is critical that the organization selects a password manager product that fulfills all these different types of security requirements while also assuring end users of the products safety. If the organization selects a product that fails to provide the required level of security the usage of the product in the organization might seize entirely and lead to additional cost due to both security issue mitigations as well as having to possibly acquire a new equivalent product.

Therefore, we can finally answer the main research question of the thesis; the most important criteria when selecting password manager software are usability and the security of the product. If either one of these criteria are not met the usage of the product within the organization is in jeopardy and the selection process could end up being a failure because the product cannot fulfill the purpose it was acquired to serve. Other criteria such as price and product features are secondary criteria to these aforementioned most important criteria and can be worked around provided that they are not significantly worse compared to what the organization is willing to accept.

7.4 Implications for practice and research

This thesis has implications for both practice as well as future research. Regarding the implications for practice, the following points should be considered by industry experts when evaluating and selecting password manager products. Firstly, one should scout and evaluate the security and technological implementation of password manager products carefully before making any commitments. This is paramount since many password manager products have been

proven to possess exploitable vulnerabilities (Silver et al., 2014; Zhao et al., 2013; Gasti & Rasmussen, 2012). Avoiding products with security issues is key especially with password manager products due to the sensitivity of the data stored in them.

Secondly, when evaluating password manager products, the usability and user experience of these types of products should be heavily weighted when comparing competing products. The importance of usability was mentioned in previous research and the empirical research (Karole et al., 2010). If a desired level of usability will not be met, it can be speculated that the desired outcomes and advantages provided by widespread usage of password manager products may not actualize.

Lastly, when evaluating and selecting password manager products, all organizations should include personnel from across the organization. This is due to the fact that individuals with different responsibilities and areas of expertise will favor certain types of evaluation criteria disproportionally due to their own interests. By having a cross organizational team evaluating password manager products, these biases can be noticed and then accounted for during the selection process of the product.

Some implications for future research also surfaced during this thesis. The purpose of this thesis was to fill a gap in existing research regarding the selection processes of password manager products in organizations. Although this study brough up some valid suggestions on how password manager products should be evaluated and selected, more rigorous research with larger sample sizes is needed in order to validate the findings of this study.

This study has studied the selection of password manager products from purely organizational and IT decision maker perspective. The end-user perspective has not been involved in this study. Future research could examine the relationship between what criteria are used to select password manager products and which of these selected products are favored by end-users.

7.5 Limitations

This study has some limitations. The empirical research of this thesis was conducted through series of qualitative interviews. It became apparent that the structure and design of the interview was not optimal, and a modified version could have produced more insightful and accurate information. One specific limitation of the interview was the factor that some of the interview questions were too open ended and left too much up for the interpretation of the interviewee and thus in some cases the interviewees interpreted the meanings of individual questions differently.

Additionally, the number of interviewees especially relating to password manager selection processes was low. Even though 12 participants took part in the empirical research process, only six participants had been involved in a process in which password manager products are evaluated and selected for or-

ganizational use. A bigger sample size would be needed in order to produce more generalizable and reliable results regarding password manager selection processes.

This thesis also studied the selection of password managers from an organizational and industry practitioner standpoint. Thus, the viewpoint of end-users is not represented in the results of the thesis. The organizational and IT expert viewpoint is merely one side of the issue and the relation between the criteria used to evaluate password managers and the end-user perception of the selected product could be examined in another instance.

The scope of the thesis was perhaps set too wide by including the topic of software selection in such great extent. This hampered the ability of the research to focus on the main topic of password manager selection on organizations. The role and scope of the topic of software selection processes should have been reduced in order to focus more on the main topic of the thesis. Even though the findings regarding software selection were useful to understand the phenomenon, it would have been beneficial to focus more on the main topic of the thesis.

Due to the coronavirus pandemic all the interviews of the empirical research process had to be conducted remotely using video conferencing software. This limited the natural interaction between the interviewer and interviewee and thus potentially impacted the empirical research process.

8 CONCLUSION

The purpose of this master's thesis was to study the phenomenon of password manager software and the selection process of password manager products in organizations. Password managers and the benefits of their usage have been widely established in previous research. However, the selection process of these software products has not yet been extensively studied. The goal of this thesis was therefore to research how the selection process of password managers functions within organizations. This goal would be achieved through the combination of a literature review into password manager software and their different aspects and an empirical research process in order to study the findings and theories that surfaced during the literature review process.

The literature review into password managers and software selection processes revealed that password manager products face some issues when it comes to their adoption and usage among individuals and within organizations. In general, it was found that users are not often aware of password manager usage benefits or are worried about the security of the product, which is not unfounded as some products contain significant security issues. Additionally, the usability of password managers turned out to be the single most significant factor in getting users to adopt password managers.

Literature review into software selection methods found that the process of software selection in organizations is a complex multi-discipline interorganizational process which is both hard to manage and presents significant impacts to the organization that is about to acquire some type of a software product. It also became apparent that the process of software selection is not extensively studied and the academic literature around the topic of software selection can be considered to be scattered.

The empirical research process found that when it comes to software selection processes it is apparent that the price and ability to fulfill business needs are the two most important criteria when organizations evaluate software products. However, rest of the results indicate that what is considered important is heavily context driven and it is hard to define any universal rules or models to guide the selection process of software products. Regarding the selec-

tion process of password manager products, usability and security repeatedly rose as the two most important selection criteria during the interview process. The importance of price was also highlighted as a secondary criterion. It became apparent that the organizational role of the person evaluating password manager software has an effect on what they consider to be important, which means that it is recommended to have individuals from across the selecting organization to evaluate these products.

The results of the empirical research process allow to answer the research questions. It was found that the most important criteria when selecting password manager products are usability and security. In relation to the supporting research questions, it was found that the selection criteria of password managers and other types of software do not significantly differ. It was also found that a list of generic software selection criteria can not be defined in a confident manner, even though some criteria seem to resurface regardless of the type of software about to be chosen or evaluated.

REFERENCES

Alanbay, O. (2005). ERP selection using expert choice software. In *ISAHP 2005*, Honolulu, Hawaii, July, 8-10

Alkaldi, N., & Renaud, K. (2016, July). Why do people adopt, or reject, smartphone password managers?. In *1st European Workshop on Usable Security*. Internet Society.

Aloul, F., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In *2009 IEEE/ACS International Conference on Computer Systems and Applications* (pp. 641-644). IEEE.

Arditi, D., & Singh, S. (1991). Selection criteria for commercially available software in construction accounting. *International Journal of Project Management*, *9*(1), 39-44.

Arias-Cabarcos, P., Marín, A., Palacios, D., Almenárez, F., & Díaz-Sánchez, D. (2016). Comparing password management software: Toward usable and secure enterprise authentication. *IT Professional*, *18*(5), 34-40.

Aurigemma, S., Mattson, T., & Leonard, L. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications?. *In Proceedings of the 50th Hawaii International Conference on System Sciences.*

Badampudi, D., Wohlin, C., & Petersen, K. (2016). Software component decision-making: In-house, OSS, COTS or outsourcing-A systematic literature review. *Journal of Systems and Software*, *121*, 105-124.

Benbasat, I., Goldstein, D. & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 11(3), 369.

Benlian, A., & Hess, T. (2011). Comparing the relative importance of evaluation criteria in proprietary and open-source enterprise application software selection–a conjoint study of ERP and Office systems. *Information Systems Journal*, *21*(6), 503-525.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *In 2012 IEEE Symposium on Security and Privacy (pp. 553-567).* IEEE.

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the

technology organization environment framework. *International Journal of Accounting Information Systems, 15(2)*, 149.

Cambridge English Dictionary (2019). Meaning of "outsourcing" in English. Retrieved from https://dictionary.cambridge.org/dictionary/english/outsourcing on 9.12.2019. Cambridge University Press.

Cheng, E. W., & Li, H. (2007). Application of ANP in process models: An example of strategic partnering. *Building and environment*, *42*(1), 278-287.

Chiasson, S., van Oorschot, P. C., & Biddle, R. (2006). "A Usability Study and Critique of Two Password Managers". *In Usenix Security (Vol. 6).*

Choong, Y. Y., & Theofanos, M. (2015). What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter. *In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 299-310)*. Springer, Cham.

Clarke, V. & Braun, V. (2017). Thematic analysis. *The journal of positive psychology, 12(3),* 297-298.

Clemons, E. K., & Chen, Y. (2011, January). Making the decision to contract for cloud services: Managing the risk of an extreme form of IT outsourcing. In *2011 44th Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information systems journal*, 8(4), 273-289.

Davis, D., Monrose, F., & Reiter, M. K. (2004, August). On user choice in graphical password schemes. In *USENIX Security Symposium* (Vol. 13, No. 2004, pp. 11-11).

Davis, L., & Williams, G. (1994). Evaluating and selecting simulation software using the analytic hierarchy process. *Integrated manufacturing systems*, *5*(1), 23-32.

De Clercq, J. (2002, October). Single sign-on architectures. In *International Conference on Infrastructure Security* (pp. 40-58). Springer, Berlin, Heidelberg.

Dhamija, R., & Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges. *IEEE Security & Privacy*, *6*(2), 24-29.

Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information systems outsourcing: a survey and analysis of the literature. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *35*(4), 6-102.

Eisenhardt, K. & Graebner, M. (2007). THEORY BUILDING FROM CASES: OPPORTUNITIES AND CHALLENGES. *Academy of Management Journal*, 50(1), 25-32.

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences, 7(1)*, 12.

Gasti, P., & Rasmussen, K. B. (2012). On the security of password manager database formats. *In European Symposium on Research in Computer Security (pp. 770-787)*. Springer, Berlin, Heidelberg.

Gonzalez, R., Gasco, J., & Llopis, J. (2010). Information systems outsourcing reasons and risks: a new assessment. *Industrial Management & Data Systems*, *110*(2), 284-303.

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, *19*(2), 213-236.

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256-267.

Gray, J., Franqueira, V. N., & Yu, Y. (2016). Forensically-sound Analysis of Security Risks of Using Local Password Managers. In *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*. IEEE, pp. 114-121.

Heckman, R. (1999). Managing the IT Procurement Process. *Information systems management, 16(1)*, 61-71.

Herley, C., & Van Oorschot, P. (2011). A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy, 10(1)*, 28-36.

Huth, A., Orlando, M., & Pesante, L. (2012). Password security, protection, and management. *United States Computer Emergency Readiness Team*.

Ion, I., Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (pp. 327-346).

Inglesant, PG., Sasse, MA. (2010). The true cost of unusable password policies: password use in the wild. In: *Proceedings of the 28th international conference on Human factors in computing systems.* (pp. 383 - 392). ACM: New York, NY, USA.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75-78.

Jadhav, A. S., & Sonar, R. M. (2009). Evaluating and selecting software packages: A review. *Information and software technology*, *51*(3), 555-563.

Karole, A., Saxena, N., & Christin, N. (2010). A comparative usability evaluation of traditional password managers. *In International Conference on Information Security and Cryptology (pp. 233-251)*. Springer, Berlin, Heidelberg.

Keil, M., & Tiwana, A. (2006). Relative importance of evaluation criteria for enterprise systems: a conjoint study. *Information Systems Journal*, *16*(3), 237-262.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., & Egelman, S. (2011). Of passwords and people: measuring the effect of password-composition policies. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2595-2604)*. ACM.

Lai, V. S., Trueblood, R. P., & Wong, B. K. (1999). Software selection: a case study of the application of the analytical hierarchical process to the selection of a multimedia authoring system. In *Information & Management*, *36*(4), 221-232.

Lang, M., Wiesche, M., & Krcmar, H. (2016). What are the most Important criteria for Cloud Service Provider Selection? A Delphi Study. In *Twenty-Fourth European Conference on Information Systems (ECIS),* İstanbul, Türkei.

Lin, H., Lai, A., Ullrich, R., Kuca, M., McClelland, K., Shaffer-Gant, J., Pacheco, S., Dalton, K. & Watkins, W. (2007, February). COTS software selection process. In *2007 Sixth International IEEE Conference on Commercial-off-the-Shelf (COTS)-Based Software Systems (ICCBSS'07)* (pp. 114-122). IEEE.

Lin, C. W., & Wang, C. H. (2011). A selection model for auditing software. *Industrial Management & Data Systems*, *111*(5), 776-790.

Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J. H. (2017, December). Analysis on the security and use of password managers. In *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)* (pp. 17-24). IEEE.

Ma, D. (2007, July). The business model of" software-as-a-service". In *IEEE International Conference on Services Computing (SCC 2007)*. (pp. 701-702). IEEE.

Mamaghani, F. (2002). Evaluation and selection of an antivirus and content filtering software. *Information Management & Computer Security, 10(1),* 28–32.

Marr, B., & Neely, A. (2003). Automating the balanced scorecard–selection criteria to identify appropriate software applications. *Measuring Business Excellence*, *7*(3), 29-36.

McCarney, D., Barrera, D., Clark, J., Chiasson, S., & Van Oorschot, P. C. (2012). Tapas: design, implementation, and usability evaluation of a password manager. *In Proceedings of the 28th Annual Computer Security Applications Conference (pp. 89-98)*. ACM.

McFarlan, F. W., & Nolan, R. L. (1995). How to manage an IT outsourcing alliance. *MIT Sloan Management Review*, *36*(2), 9.

Ngai, E. W., & Chan, E. W. C. (2005). Evaluation of knowledge management tools using AHP. In *Expert systems with applications*, *29*(4), 889-899.

Nowell, L. S., Norris, J. M., White, D. E. & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International journal of qualitative methods, 16(1)*

Oliveira, T., & Martins, M. F. (2010). Information technology adoption models at firm level: review of literature. In *The European Conference on Information Systems Management* (p. 312). Academic Conferences International Limited.

Pashalidis, A., & Mitchell, C. J. (2003, July). A taxonomy of single sign-on systems. In *Australasian Conference on Information Security and Privacy* (pp. 249-264). Springer, Berlin, Heidelberg.

Repschlaeger, J., Wind, S., Zarnekow, R., & Turowski, K. (2012). Selection criteria for software as a service: an explorative analysis of provider requirements. *AMCIS 2012 Proceedings*. Paper 3.

Saaty, T. L. (1990). How to make a decision: the analytic hierarchy process. *European journal of operational research*, *48*(1), 9-26.

Sahay, B. S., & Gupta, A. K. (2003). Development of software selection criteria for supply chain solutions. *Industrial Management & Data Systems*, *103*(2), 97-110.

Silver, D., Jana, S., Boneh, D., Chen, E., & Jackson, C. (2014). Password managers: Attacks and defenses. *In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 449-464)*.

Stobert, E., & Biddle, R. (2015). Expert password management. *In International Conference on Passwords (pp. 3-20)*. Springer, Cham.

Summers, W. C., & Bosworth, E. (2004). Password policy: the good, the bad, and the ugly. *In Proceedings of the winter international symposium on Information and communication technologies (pp. 1-6)*. Trinity College Dublin.

Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In *21st Annual Computer Security Applications Conference (ACSAC'05)* (pp. 10-pp). IEEE.

Tam, M. C. Y., & Tummala, V. M. R. (2001). An application of the AHP in vendor selection of a telecomuunications system. *Omega, 29(2)*, 171–182.

Walkup, E. (2016). The password problem (No. SAND2016-5208T). *Sandia National Lab.(SNL-NM)*, Albuquerque, NM (United States).

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. *In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (pp. 175-188).*

Zhao, R., & Yue, C. (2014). Toward a secure and usable cloud-based password manager for web browsers. *Computers & Security, 46*, 32-47.

Zhao, R., Yue, C., & Sun, K. (2013). Vulnerability and risk analysis of two commercial browser and cloud based password managers. *ASE Science Journal, 1(4*), 1-15.

APPENDIX 1 INTERVIEW STRUCTURE

Background questions

- What is your main discipline/ area of expertise?
- How long is your experience in IT?

Software selection

- Have you participated in processes/projects in which software products are selected for an organization?
    - Yes -> ask the interviewee to consider the last or any notable project they had been a part of in which a software product was selected to be used within an organization
        - Why was the specific product chosen over the other competing products?
        - Can you single out any specific factors and criteria that the selected product was better in in comparison to its competitors?
    - No -> skip the question and move on
- What would you consider to be the three overall most important selection criteria when it comes to selecting software products?
- Please state how important you consider the following software selection criteria to be in scale from 1-5, where 1 = not important at all and 5 = very important.
    - ○ Cost
    - ○ Flexibility
    - ○ Combability / integration
    - ○ Customization
    - ○ Usability
    - ○ Support & Service
    - ○ Backups/Contingency
    - ○ Vendor
    - ○ Ease of initial deployment
    - ○ Security
    - ○ Features/Functionality
    - ○ Stability & Availability & Reliability
    - ○ Scalability
    - ○ Technical specifications
- Did I miss any important criteria?
- Did you utilize any defined models or theories in the process of selecting software products?
    - Yes
        - What models did you utilize?
        - Were these models useful in your decision-making process?
    - No

    - Do you think you could benefit from established models or frameworks when comparing software products?

Password manager selection

- Do you personally use a password manager?
- What factors and features do you consider important in password manager software?
- Have you participated in a process/project in which password manager software is selected for an organization?
    - Yes
        - Why was the one product chosen over all the others?
        - Do you think the selection was successful?
    - No
        - Skip the question and move on
- In the context of selecting a password manager product, please state how important you consider the following criteria to be in scale from 1-5, where 1 = not important at all and 5 = very important.
    - Cost
    - Flexibility
    - Combability / integration
    - Customization
    - Usability
    - Support & Service
    - Backups/Contingency
    - Vendor
    - Ease of initial deployment
    - Security
    - Features/Functionality
    - Stability & Availability & Reliability
    - Scalability
    - Technical specifications
- Did I miss any important criteria?

Interview end.