The Influence of Risk Factors in Decision-making Process for Open Source Software Adoption

Pre-print

To cite:

Silic, M., & Back, A. (2015). The Influence of Risk Factors in Decision-Making Process for Open Source Software Adoption. International Journal of Information Technology & Decision Making, 1-35

Mario Silic,

University of St Gallen,
Institute of Information Management, Switzerland
Zagreb School of Economics and Management, Croatia
mario.silic@unisgh

Andrea Back

University of St Gallen,
Institute of Information Management, Switzerland
andrea.back@unisg.ch

Research paper

Abstract

"Nobody ever got fired for buying IBM," was a widely used cliché in the 1970s in the corporate IT (information technology) world. Since then, the traditional process of purchasing software has dramatically changed, challenged by the advent of open source software (OSS). Since its inception in the 1980s, OSS has matured, grown, and become one of the important driving forces of the enterprise ecosystem. However, it has also brought important IT security risks that are impacting the OSS IT adoption decision-making process. The recent Heartbleed bug demonstrated the grandeur of the issue. While much of the noise relates to the amplification of perceived risks by the popular mass media coverage, the effect is that many enterprises, mainly for risk reasons, have still chosen not to adopt OSS. We investigated "how do information security related characteristics of OSS affect the risk perception and adoption decision of OSS" by conducting an online survey of 188 IT decision-makers. The proposed Open Source Risk Adoption Model offers novel insights on the importance of the perceived risk antecedents. Our research brings new theoretical contributions, such as understanding the perceived IT security risk relationship with adoption intention in the OSS context, for researchers and important insights for IT information professionals. We have found that IT security risk has a significant role in OSS adoption intention. Our results offer possible future research directions and extend existing theoretical understanding of OSS adoption.

Keywords: Risk factors, Information security, Organizational security, Open Source Software, IT Risks

1 Introduction

"Nobody ever got fired for buying IBM" was a widely used cliché in the 1970s in the corporate IT (information technology) world. The traditional process of purchasing software by acquiring its license did not have any alternative until 1998, when the open source phenomenon appeared. Until then, software was seen as a product that we have to pay for, just like we would for any other material object (Schryen, 2011). The open source movement led to the birth of open source software (OSS) (Perens, 1999). "OSS" means that the source code is freely available and can be adapted to match potential new needs. It is often defined as software that can be freely modified, freely distributed, is technologically neutral, and grants free subsidiary licensing rights (Perens, 1999). In today's modern economies, organizations have the choice between acquiring software by paying for its license, building customized software or adopting an OSS product that is free of charge. In this context, software adoption is seen in large part as a risk-driven process (Shaikh & Cornford, 2012). Indeed, in the OSS case, the open source community, responsible for the design, development, and maintenance of an OSS project may disband and thus impact the future of the project itself (Germonprez et al., 2012). Many other risks present in the OSS context have been identified in past research: security risks (Herbsleb, 2002), lack of expertise (Krishnamurthy, 2003), compatibility (Guth, 2006), ownership (Kenwood, 2001), or training issues (Forrester, 2004). Many of these risks stem from the infancy or instability of an open source community, which fails to provide real value to organizations when compared to proprietary solutions. A study from (Schweik & English, 2012) found that out of 145,475 projects from the popular OSS portal Sourceforge.org, 46% were abandoned in the initiation stage and only 17% were successful (one of the successful project common characteristic is a "relatively clearly defined vision and a mechanism to communicate the vision early in the project's life"). The reasons behind these significant numbers of failures in the OSS project lifecycle lay in the origins of the OSS model, which was conceived on the foundations of freedom (freedom to run, copy, distribute, study, change, and improve software) and choice (choice to distribute your version or not) (Scacchi, 2007). But freedom and choice introduce risks (Gartner, 2011). The risks that are introduced may have disastrous consequences leading to expensive failures (Franch et al., 2013). The lack of good risk management was highlighted as one of the key points to take into consideration when implementing an OSS product (Gartner, 2011).

OSS enterprise adoption is booming with some software segments, such as the web server market; OSS technology is the leader in server software count (e.g. Netcraft, 2014) a web server survey found that 54% of all worldwide servers are using an OSS product such as Apache or nginx). Also, Strategyanalytics

(2013) announced that the Android operating system (an OSS product) reached a new record of 81% global share in smart phone market. These facts would suggest that in the enterprise context, OSS is being broadly adopted. However, it seems that enterprises are more cautious when it comes to OSS adoption. This is partly explained by the fact that enterprises are not performing any real cost-benefit analysis (Ven, Verelst, & Mannaert, 2008). In other words, the OSS evaluation process can be very time consuming and heavy and these hidden costs are just one of the potential technological risks (Tiangco, Stockwell, Sapsford, Rainer, & Swanton, 2005). In order to minimize these risks, often, it is necessary to go through the phase of end-user training (Morgan & Finnegan, 2007a) and getting the professional support (Fitzgerald & Kenny, 2004). The quality of the OSS product was also questioned by researchers (Fitzgerald & Kenny, 2004; Rudzki, Kiviluoma, Poikonen, & Hammouda, 2009; Ven et al., 2008) along with issues of 'compatibility' and 'lack of standards' (Ågerfalk, Deverell, Fitzgerald, & Morgan, 2005; van Rooij, 2007). Several study findings have revealed that enterprise adoption of OSS is still minimal. For instance, a CNBC (2013) report indicates that the closed-source software iOS is still the predominant operating system for tablets used at work, with 55% of the market share compared to 25% of the market share for Android. Also, according to a Hubspan (2011) survey, Linux has only 9% of the market share for enterprise desktop operating systems. This slower enterprise OSS adoption trend is mostly explained by the fact that quality and security have been important topics of dispute and debate between the open and closed source opponents (Gartner, 2014). From an enterprise perspective 64% of enterprises still view security as a major obstacle to OSS adoption (Deloitte, 2012). In this study, we follow ISO's definition of security risk which defines it as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" (ISO, 2008). Harm usually leads to several different risks for organizations that are, ultimately, all about the financial, reputational or legal consequences that organizations look to avoid. More precisely, in the OSS context the IT security risk can be related to, for instance, hidden costs (e.g. time spent performing an OSS evaluation can be very lengthy).

Overall, past research has studied different potential risks behind OSS adoption, but most of these studies face generalizability challenges since either they were focusing on a single (specific) OSS product in a particular organization/country (Goode, 2005) or their research setting was public administration (Federspiel & Brincker, 2010) and software companies (Hauge, Ayala, & Conradi, 2010). Indeed, because Ven and Verelst (2012) found that research in this area is still fragmentary and the corresponding results are inconclusive, it has led to ambiguity about the factors that influence decision-makers.

Therefore, we are missing a holistic view of the perceived IT security risk factors that influence the IT executive's adoption decisions. Management of IT security risks in the OSS adoption context implies the use of specific risk management procedures and policies aimed at risk reduction. The goal of this research paper is to analyze the management of IT security risk in the context of OSS adoption practices by explaining and providing factors that help reduce perceived risk in the IT executive's decision-making process. We aim to answer the following research question: How do information security related characteristics of OSS affect the risk perception and adoption decision of OSS?

We believe that better understanding the IT security risks related to OSS is of the highest importance and that it has not received adequate research focus thus far. To fill this research gap, our study aims to investigate the perceived risk factors that influence the enterprise adoption intention in the context of OSS. This paper will introduce the Open Source Risk Adoption model, which will provide theoretical foundations for OSS adoption. Furthermore, we will explain the underlying risk factors and how they correlate with the decision-making process during OSS adoption. Finally, besides the risk context we highlight, this paper will also contribute to the ongoing openness phenomenon where organizations are uncontestably looking for. The paper is structured in the following way. First, we risk phenomenon in Section 2.1. Second, in the literature review sections 2.2 and 2.3 we review past research on open source software and risk and technology adoption, and understand how other scholars have approached the topic. Finally, we will present our methodology (Section 3), research results (Section 4), and discuss our findings (Section 5) after what we conclude (Section 6).

2 Literature Review

In this section, we will review the literature on OSS, and consumer technology adoption.

While OSS brings clear advantages for enterprises, such as cost cuts through reduced scaling costs, license fees, hardware needs, etc. (Fitzgerald & Kenny, 2004; Schweik & English, 2012), OSS adoption still raises important IT security risks in the enterprise context. Some of these IT security risks are related, for instance, to spurious open source software, where anonymous programmers with bad intentions modify the original source code and embed malicious code into the original distribution (Sans, 2009). For example, in 2012, a security incident affected piwik (popular open source web analytics application) and malicious code was embedded that affected over 480,000 websites.

Another incident in 2012 involved phpMyAdmin (database administration tool used by over 15 million system administrators), where malicious code was placed on one of the official mirrors of the Source

Forge site. More recently, in 2014, the Heartbleed security bug found in the open source OpenSSL product affected all major websites, including Google, Facebook, Yahoo, etc. The results from these security incidents has been high media coverage, where the OSS product is usually marked as being vulnerable, insecure, and potentially dangerous for enterprises (e.g. PC World, 2014; The Register, 2013). As a consequence, many enterprises are still reluctant to adopt an OSS product because IT executives are unsure if, and to what extent, they can trust OSS (Del Bianco, Lavazza, Morasca, & Taibi, 2011). However, the issue of trust is not just related to OSS. It is a general software issue. According to Kou, Shi, and Dong (2012): "Developing software systems that can be justifiably trusted are of enormous significance ". Consequently, quite often, it is not the actual IT security risk that impacts IT executives' decision-making process, but rather the perceived risk that IT executives incorporate into their adoption decisions factors. In other contexts, it was found that the perceived IT security risk often seems to be a critical decision-making factor. For example, in the cloud computing context, the risks and challenges that have been introduced from the relocation to the clouds are prevalent when the decision to migrate or not has to be taken (Zissis & Lekkas, 2012). Overall, it is argued that software development as a process brings plenty of risks where detection of the errors present in software modules is not only difficult objective to achieve (Peng, Kou, Wang, Wang, & Ko, 2009), but also to find the good method to predict the errors (Kou, Peng, Shi, & Wu, 2012) that can be found, for instance, when conducting financial risks analysis (Kou, Peng, & Wang, 2014).

Better understanding the perceived IT security risks related to OSS adoption is an important aspect in the business decision-making process. Knowledge about the associated risks and their better management would allow faster, better, and easier integration of an OSS product into an enterprise's information systems. So far, scholars have mostly focused on the IT security-related risks of one single OSS product or just a few OSS products only (Alhazmi, Malaiya, & Ray, 2007; Browne, Arbaugh, McHugh, & Fithen, 2001; Frei, May, Fiedler, & Plattner, 2006; Neuhaus, Zimmermann, Holler, & Zeller, 2007).

2.1 Risk Management

The word "risk" comes from ancient Italian word "*risicare*," which means "to dare," and in that context it can contain negative as well as positive connotations (Wolke, 2008). Risk management as a discipline started to be studied only after World War II (Dionne, 2013). For a long time, risk management has been synonymous with market insurance, aiming at individual and organizational protection against potential losses from accidents (Harrington & Niehaus, 1999).

In information systems research (ISR), risk management appeared with the birth of the information system (IS) itself, which is composed of various assets such as hardware, software, data, people, and infrastructure (Sun, Srivastava, & Mock, 2006). These organizational assets are often compromised by threat agents. Threat agents can include any external or internal threats (e.g. hackers, competition, and employees) that are looking to exploit and abuse organizational assets; however organizations, at the same time, are putting countermeasures in place to reduce risk. It should be noted, though, "residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents representing a residual level of risk to the assets" (Infrastructure & Profile, 2002). Overall, IS risk management is a complex area that explains why, currently, there is no consensus on the definition of "risk." In most IS studies, risk is defined using a negative deviation and as such, it is focused on avoiding losses. According to Purdy (2010) "it is now widely understood that risk is simply a fact of life and is neither inherently good nor inherently bad ". We also support this view that risk cannot be simply viewed as something good or bad.

Contrary to the actual risk, the perceived risk is usually defined as the feeling of uncertainty about the negative outcomes when adopting a new product (Cunningham, 1967). According to Cunningham (1967) the perceived risk may lead to an expected loss and as such its importance is vital in the decision-making process, where the entire process is surrounded by uncertainty, anxiety, and conflict that affects the decision-maker (Bettman, 1973). Risk assessment is an important phase that can result in an overestimation of risks (e.g. Gregory and Mendelsohn (1993)) or an underestimation of risks (e.g. Rhee, Ryu, and Kim (2012)) where several limitations (e.g. low level of management awareness about security threats) impact the decision-maker. Koller (1988) argues that the severity level of perceived risk will be higher if possible negative consequences have higher impact on organizational assets. This is in line with the mathematical risk definition (e.g. Boehm (1981)). Consequently, we define perceived risk as "the potential for loss in the pursuit of a desired outcome" (Featherman & Pavlou, 2003).

Information technology emerged as an important area within organizational IS, bringing new value to organizations and transforming their business procedures, processes, and products (Porter & Millar, 1985). The definition of IT security risk management (ISRM) is usually described and defined as a cyclical model that has four phases: identification, quantification, controlling, and monitoring Faisst and Prokein (2005). These four phases can be extended to seven phases (resource profiling, risk assessment, risk evaluation, document, risk mitigation, validation and monitoring and audit) (Wheeler & Swick, 2011). Often, IT security risk management is seen as an ongoing process where identification and prioritization

of the IT security risk is necessary, with the objective to implement and monitor controls, countermeasures, and safeguards that will address and reduce those potential risks (Spears & Barki, 2010). Business strategy, which feeds various business processes, provides guidelines on the implementation of effective and efficient ISRM (Culp, 2002). Generally speaking, ISRM is part of the wider enterprise risk management (ERM) process and as such, it has two objectives: 1) to assess security risks and 2) to select protection measures to reduce security risks (Yue, Çakanyıldırım, Ryu, & Liu, 2007). According to Whitman and Mattord (2013), the activities that ISRM has to support are risk identification, risk analysis, and risk control. Each of these activities supports different tasks, such as, for example: 1) security measure identification (risk identification), 2) vulnerability analysis (risk analysis), and 3) acceptable risk assessment (risk control). Typically, this risk-related task flow would be used in the software context, where vulnerabilities are often found (Yue et al., 2007).

Another important aspect that ISRM has to deal with is risk communication, which has to inform all organizational stakeholders about the risk processes (Fischhoff, 1995) in order to have a common understanding of all risk-related aspects. Other aspects, such as organizational culture, can influence the awareness of threats. For example, Bozeman and Kingsley (1998) found, when comparing public and private organizations, that there is considerable variance in an organization's risk culture and that variance can affect the overall risk. Generally, there are several generic frameworks that define risk management methodology. The most popular one is ISO 27005[1] and consists of: context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review. The common goal for all these different layers is to avoid potential loss for the enterprise. And that can be done only through the proper identification of assets, threats, vulnerabilities, risk mitigations, and possible consequences.

Recently, risk management methodology has been criticized for being shallow (Vacca, 2012). Claims have been made that it focuses more on guessing rather than predicting the future on the basis of statistical evidence. Despite the critique, there is currently no better alternative.

As we can see from the above, risk management is a highly complex field characterized by numerous technological advances that are impacting the way enterprises are looking at underlying risks.

2.2 Risk and Open Source Software

[1] See http://www.iso.org/iso/catalogue_detail?csnumber=56742 for more information.

OSS adoption has several potential risks. One such risk is that organizations often fail to perform any cost-benefit analysis that precedes an enterprise's OSS adoption (Ven et al., 2008). Hidden costs are one of these potential risks where the time spent performing an OSS evaluation can be very lengthy (Tiangco et al., 2005), with the need to have user training (Morgan & Finnegan, 2007a) and professional support (Fitzgerald & Kenny, 2004). The quality of OSS products has also been questioned by researchers (Fitzgerald & Kenny, 2004; Rudzki et al., 2009; Ven et al., 2008) along with their "compatibility" and "lack of standards" issues (Ågerfalk et al., 2005; van Rooij, 2007). Licensing represents another challenge as a number of different types of licenses do exist (McGhee, 2007; Tiangco et al., 2005) and they do not facilitate the product's integration with an enterprise's existing proprietary licenses (Jaaksi, 2007). Another important risk relates to the lack of expertise and support. Others face challenges with documentation or a roadmap (Ågerfalk et al., 2005) that may be a hindering factor in their adoption (Hauge et al., 2010).

Overall, we can see that researchers have studied different potential risks behind OSS adoption, but most of these studies face generalizability challenges as either they focused on a single (specific) OSS product in a particular organization/country (Goode, 2005) or their research setting was public administrations (Federspiel & Brincker, 2010) and software companies (Hauge et al., 2010). As such, they may not offer a holistic view on the perceived IT security risk when adopting OSS. Indeed, for Ven and Verelst (2012) research in this area is still fragmentary and the corresponding results are inconclusive, which leads to ambiguity about the factors that influence the decision-makers. Interestingly, only few studies have been concerned with studying the organizational adoption of OSS (Ven & Verelst, 2012). Consequently, for decision-makers, it is very difficult to clearly see and understand which factors and criteria they should be basing their decisions on (Ven et al., 2008).

The debate over the security of open source vs. closed-source software is still on going and past research has not come to any clearer conclusions. For Payne (2002), open source is not more secured than closed-source software. However, Schryen (2009) argues that this debate is often driven by biased attitudes where there is a lack of quantitative data to support the results. By comparing the published vulnerabilities of open- and closed-source software, Schryen (2009) concluded that there is no significant difference in the severity levels between open- and closed-source software. However, one limitation of the studies that compare IT security risk between open- vs closed-source software is the number of cases used for comparison, which is generally very low. Another one is the fact that the

majority of these studies are already outdated (produced between 2005 and 2009) and may not reflect the recent OSS expansion in terms of new OSS products (e.g. big data, mobile, and cloud).

Research also indicates that trust in the open source development process is very important as there is a risk of opportunistic behavior by unknown developers (Hissam, Plakosh, & Weinstock, 2002; Stewart & Gosain, 2001). Also, the distrust concerning OSS quality is another argument for rejecting OSS products (Laplante, Gold, & Costello, 2007). In this context, discovering the risk factors that influence the IT decision-making process would be beneficial for enterprise OSS adoption (Morgan & Finnegan, 2007b). A survey based on OSS's trustworthiness identified functionality and reliability as key factors that influence trust in OSS from users and developers (Del Bianco et al., 2011). While the literature analysis reveals that trustworthiness in an OSS product is positively impacted by several factors such as reliability (Ven & Verelst, 2012), user satisfaction (Eryilmaz, Cochran, & Kasemvilas, 2009), audit (Cowan, 2003) and expertise (Chou & He, 2011). Hence, we are missing a more complete overview of IT security risk factors that influence the trustworthiness of an OSS product from an enterprise perspective.

Hence, if enterprises want to take full advantage of OSS adoption, it is necessary to understand and manage all the risks since they directly influence business decisions Furthermore, Franch et al. (2013) argue that the business model that brings new value propositions based on OSS may fail because business risks will be overlooked.

Moreover, past literature reveals that researchers focused mainly on OSS benefits, praising its advantages, such as reduced avoidance of vendor lock-in (Shaikh & Cornford, 2012) or cost savings (Nagy, Yassin, & Bhattacherjee, 2010). However, for (Hauge et al., 2010; Nagy et al., 2010), the IT security risks related to OSS adoption are not yet well understood, and research that is conducted in a more systematic way would bring more precision, accuracy, and generalizability to the results.

2.3 Organizational Adoption of OSS

Technology acceptance is one of the most well studied areas in IS research. Several technology acceptance models have been developed in the last decade to explain the theoretical background of technology acceptance and use. Organizational technology adoption seeks to understand the factors that influence the organizational adoption decision on information technology (Fichman, 2000). While many researchers have tried to propose a universal theory on organizational technology adoption (Kwon & Zmud, 1987), this theory is still nonexistent. There are several different theories that explain

technology adoption. In this research project, we will use the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980).

This intention model is particularly useful to understand the behaviors and intentions that decision-makers may have in the context of OSS, as their decisions will be influenced by salient positive and negative beliefs about an OSS product. Several other studies confirmed this relationship between the intention to increase adoption and the negative impact of perceived risk (e.g. Benlian & Hess, 2011a; Gewald & Dibbern, 2009). The TRA appeared in the late 1960s with the objective to help researchers in better understanding the attitudes and behaviors of individuals. The model suggests that behavioral intention is determined by an individual's behavior and his decision to engage in a specific behavior. Furthermore, the theory argues that behavioral intention to act is composed of the attitude toward a given behavior and the motivation to comply with these beliefs (Ajzen & Fishbein, 1980).

Past studies using TRA as a theoretical foundation to understand decision-makers' attitudes toward their behavioral intentions have been quite successful (e.g. Madden, Ellen, & Ajzen, 1992). Following Benlian and Hess (2011b), we intend to understand how decision-makers' attitudes toward OSS are influenced by salient behavioral beliefs. In other words, decision-makers will take into account the positive and negative attitudinal appraisals when evaluating an OSS product, which will influence their adoption intention. Hence, OSS product adoption will be strongly influenced by the decision-maker's evaluation of the positive and negative utility in connection to the OSS. Past research did confirm this relationship, showing that perceived risk (or negative utility) strongly impacts the decision-maker adoption process (e.g. Featherman & Pavlou, 2003) and that perceived benefits (positive utility) positively affect the decision-maker intention with regard to the IT adoption process (e.g. Gewald & Dibbern, 2009).

To frame OSS adoption in theory is not an easy task, as the existing literature shows that the factors that influence OSS adoption are rather complex and subjective (Dedrick & West, 2003; Fitzgerald & Kenny, 2004). Moreover, we lack a valid and generalizable framework to better understand and model OSS adoption from Macredie and Mijinyawa (2011). Past studies have shown that the perceived benefits and drawbacks of OSS are the contributing factors to its adoption. Some of the perceived benefits were identified as follows: reliability (Varian & Shapiro, 2003), security (Forge, 2006), performance (Kenwood, 2001), vendor lock-in (IDC, 2004), innovation (Wheeler & Swick, 2011). On the perceived drawbacks, several factors were found to be important for OSS adoption: security risks (Herbsleb, 2002), lack of expertise (Krishnamurthy, 2003), compatibility (Guth, 2006), ownership (Kenwood, 2001), and training

considerations (Forrester, 2004). Overall, researchers have identified a wide range of different factors that influence the organizational adoption decision regarding OSS. Furthermore, for Li, Tan, and Yang (2013), experimenting with OSS in organizations can be dangerous because OSS brings risks in terms of security and maintenance, with a unique development style where support and services may be missing. One limiting factor of the previous studies is that they mostly used a case study approach involving a limited number of organizations (Ven & Verelst, 2012); such an approach often leads to inconclusive or contradictory results (Ven et al., 2008).

Overall, in line with the TRA, we argue that a decision-maker's intention to adopt an OSS product will depend on his attitude toward OSS with regard to how the increased adoption will be negatively associated to the perceived risks. Moreover, the TRA supports an active decision-making process, which provides a good theoretical fit for our research. Finally, the perceived IT security risk is an important factor that plays a crucial role in the decision-making process since it affects positive and negative attitudes that are key to behavioral adoption intentions. Therefore, we use the risk antecedents to the OSS context, and by using an adapted trust-theoretic model (Srivastava, Chandra, & Theng, 2010), we propose our research model as described in Section 3.

3 Research Model and Hypotheses

Previous literature on risk perception provides three major dimensions that affect perceived IT security risk (PISR) in the OSS context, addressing: perceived lack of confidentiality, perceived lack of integrity, and perceived high availability (Benlian & Hess, 2011b; Featherman, Valacich, & Wells, 2006; Gewald, Wüllenweber, & Weitzel, 2006; Kim, Ferrin, & Rao, 2008; Peter & Tarpey Sr, 1975). Furthermore, we also add a perceived high structural assurance dimension (McKnight, Choudhury, & Kacmar, 2002). These four characteristics (Figure. 1) are identified as the main factors that affect perceived risk in OSS technology.

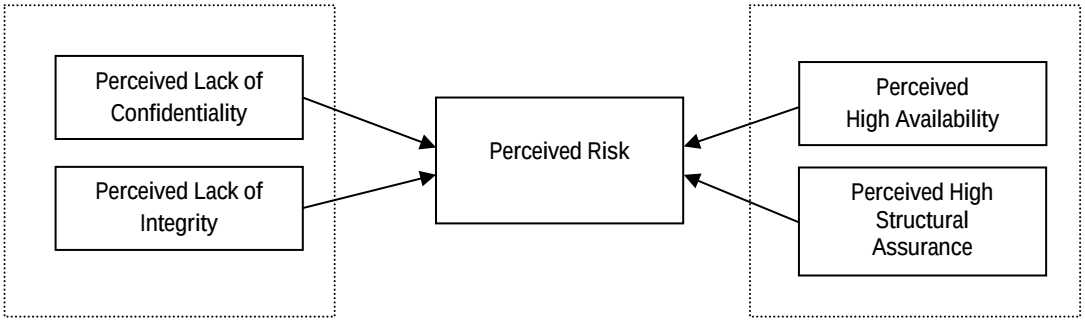

Figure 1: Factors Affecting Perceived IT Security Risk in the OSS Context

The CIA triad (confidentiality, integrity, and availability) is one of the core principles of information security, which is a risk management discipline whose job is to manage the cost of information risk to a given business (Blakley, McDermott, & Geer, 2001). Information security (InfoSec) is often defined as the protection and preservation of confidentiality, integrity, and availability of information (ISO, 2008).

- Perceived lack of confidentiality (PC) defines the situation where security-relevant elements are only known to a defined circle of people. It is about the potential loss of privacy impacting organizational data. It deals with unauthorized access to information. One example is data leakage caused by a malicious OSS product. It is usually controlled with encryption and authentication methods.
- Perceived lack of integrity (PI) risk is present when information is no longer certain to be reliable or accurate. It is about the data integrity, where data could have been changed inappropriately by accident or by malicious activity. For example, changing the source code of an OSS product for malicious reasons can affect data integrity. Integrity is compromised when any type of unauthorized change to information in transmission, storage, or processing is involved (Amoroso, 1994).
- Perceived high availability (PA) defines the availability of a system and its ability to deliver the requested services (Pressman & Jawadekar, 1987). It can be expressed as the ratio of time a system is functional to the total time it required to function (e.g. 90%).
- Perceived high structural assurance (PSA) refers to a consumer's perception about the institutional environment where technology use is safe, reliable, and secure. It refers to different technological safeguards and structures that should provide good assurance when using the technology. Assurance can be accomplished by providing encryption, authentication, firewalls, digital signatures, privacy seals, and third-party certifications (Aldridge, White, & Forcht, 1997; Garfield & McKeown, 1997; Ratnasingham, 1998).

Also, following the TRA, we introduced two other dimensions: perceived negative utility (i.e. perceived loss or cost) and perceived positive utility (i.e. perceived benefits).

On the one hand, perceived negative utility (PNU) can be explained as "the felt uncertainty regarding the possible negative consequences of adopting a product" (Benlian & Hess, 2011a). Consequently, the perceived negative utility dimension can be used in the OSS adoption context where a decision-maker is

uncertain about his decision (Bettman, 1973). Hence, in this paper, PNU is defined as the potential for loss when adopting an OSS product.

On the other hand, the perceived positive utility (PPU) brings opportunities and benefits that have a much stronger influence on the adoption process (Benlian & Hess, 2011b; Gewald & Dibbern, 2009). Thus, we defined PPU as the potential for gain when an OSS product is adopted. From an organizational standpoint, PPU will be seen as a positive strategic option that brings opportunities and benefits.

3.1 Research Model

In Figure 2, we present our research model. It shows that perceived risk plays an essential role in Adoption Intention (AI).

3.2 Research Hypotheses

Relationship Between Perceived Risk, Perceived Lack of Confidentiality, Perceived Lack of Integrity, Perceived High Availability, and Perceived High Structural Assurance

The loss of privacy represents one of the main concerns during the adoption of a new product or service where the protection of information is crucial (Featherman & Pavlou, 2003; Kim et al., 2008). Confidentiality is linked to the OSS product's reputation. Certainly, "Reputation has an economic value" (Hill, 1990), and it plays an important role in defining the willingness of others to engage in a transactional relationship. However, reputation results from trustworthy behavior. Thus, the perceived risk will be positively associated with the level of the perceived lack of confidentiality offered by an OSS product. Consequently, if perceived lack of confidentiality is high, then it may result in having perceived risk level higher. For McKnight et al. (2002), reputation builds trust: "When users first experience technology, signals of well-done user interfaces and good vendor reputations will build trust. Reliable, dependable, quality IT performance is the key over time . . . the entire system infrastructure should demonstrate quality." Thus, we hypothesize:

> *H1: IT decision-maker beliefs regarding perceived lack of confidentiality risks will have a negative impact on perceived low risk.*

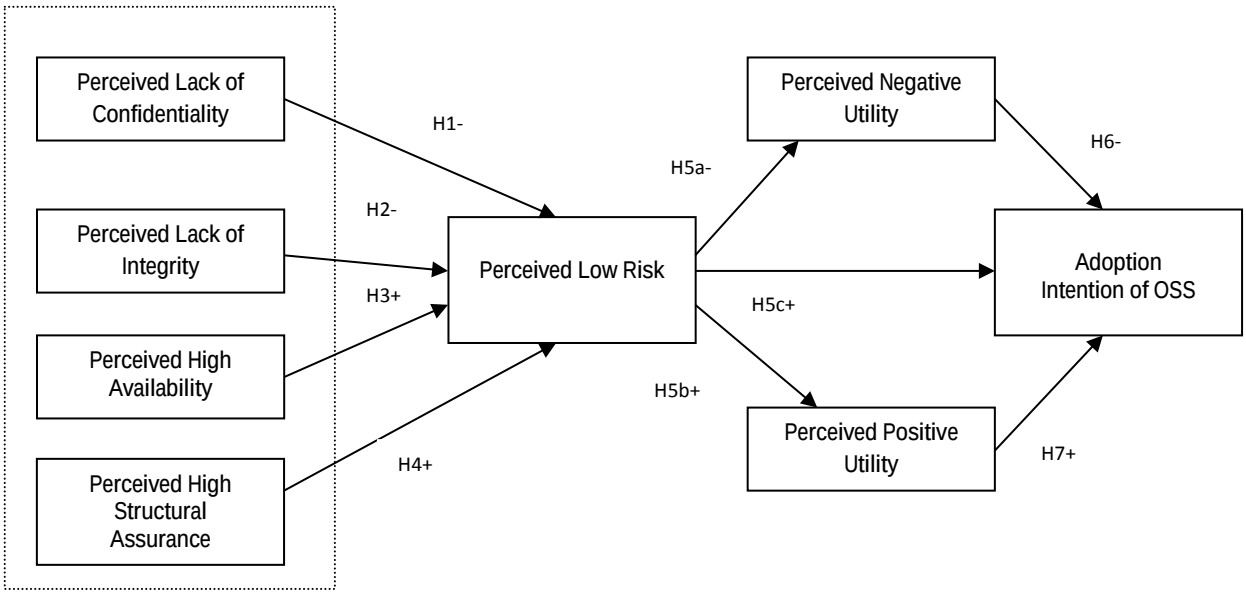

Figure 2: OSS Adoption Research Model

For Williamson (1975) integrity is the opposite of having a ‘‘lack of candor or honesty in transactions, to include self-interest seeking with guile.” Clearly, it leads to the situation of opportunism that includes not only blatant forms of cheating, but also the less obvious yet clearly calculated methods of misleading, distorting, disguising, and confusing actions people sometimes take (Hill, 1990). Integrity is about fairness, justice, consistency, and the fulfillment of a promise and is usually defined as the extent to which a trustee is believed to adhere to ethical principles (Colquitt, Scott, & LePine, 2007). Consequently, integrity will negatively influence perceived risk if others know about the organizational information or when technology makes certain promises without fulfilling them. Thus, we hypothesize:

> *H2: IT decision-maker beliefs regarding perceived lack of integrity risks will have a negative impact on perceived low risk.*

Ensuring access to information when it is needed is the objective of every service provided by an OSS product. For example, the Linux web server has an overall good reputation for being reliable in delivering requested services. Poor availability would lead to potential financial losses. Without dependable availability, customers would lose confidence, which could lead to an increased risk. Several past studies, in other contexts, have confirmed that when availability is adequately provided, the perceived risk will decrease (Pavlou, Huigang, & Yajiong, 2007b). Thus, when an IT decision-maker decides on an OSS product adoption, availability perception could be an important evaluation criterion to take into account. Thus, we hypothesize:

H3: IT decision-maker beliefs regarding perceived high availability risks will have a positive impact on perceived low risk.

Perceived high structural assurance (PSA) is the perception about the entire OSS environment where different structures such as guarantees, promises, compliance and legal will provide safe, secure, and reliable operations. OSS technology has an important dual-use (technology that can be used for both helpful and harmful purposes), where content of the OSS may be malicious or flawed and as such can represent security risk for organizations (Silic, 2013). When introduced in the organizational ecosystem, its intentions may not always be honest and fair, since organizations rely on the programming results of mostly anonymous strangers in cyberspace, where the issue of trust is omnipresent (De Laat, 2010). Data encryption or application authentication measures can help decision makers to rely on these structural assurance techniques and feel more comfortable in their decision making process. As a result, it is possible to prevent or reduce privacy and financial losses to a minimum (McKnight et al., 2002). Furthermore, any other legal or compliance structures can help to ensure the right level of perceived risk. Confidence in the technological safeguards of OSS technology could be another factor influencing perceived risk. Thus, we hypothesize:

H4: IT decision-maker beliefs regarding perceived high structural assurance will have a positive impact on perceived low risk.

Relationship between Perceived Risk, Perceived Negative Utility, and Perceived Positive Utility (PPU)

Perceived negative utility refers to situations where an IT decision-maker is uncertain about his decisions and feels uncomfortable in making a decision. Such a situation is increasing anxiety (Bettman, 1973). Hence, PNU can be seen as the potential for loss in the IT decision-making process. In past studies, the perceived risk is highlighted as one of the main factors affecting organizational behavior when it comes to risks associated with IT adoption (e.g. Benlian & Hess, 2011b; Featherman & Pavlou, 2003). The study exploring the business process outsourcing phenomenon among German banks, found that performance and privacy had a high effect on the overall perceived risk (Gewald & Dibbern, 2005). Consequently, we expect that lower perceived risk will have a negative impact on the perceived negative utility. Thus, we hypothesize:

H5a: Lower perceived risk will result in lower perceived negative utility.

It is also likely that perceived positive utility will be positively impacted by the perceived risk. Indeed, PPU is about the perceived benefits that an OSS product brings and these benefits may be positively impacted if the perceived risk is lower. More precisely, if an IT decision-maker has low perceptions about potential IT security risks, then his assessment of an OSS product may be strongly influenced in a positive way by maximizing any possible benefits. This will then impact the existing benefits related to, for example, the switching cost from a proprietary solution to an open source one, where higher switching costs can be expected (Bonaccorsi & Rossi, 2003). Finally, a number of previous studies did identify the positive relationship between perceived risk and perceived usefulness, which results in an increased adoption intention (e.g. Carter & Belanger, 2005; Fang, Chan, Brzezinski, & Xu, 2005; Featherman & Pavlou, 2003). Thus, we hypothesize:

H5b: Lower perceived risk will result in greater perceived positive utility.

Finally, risk was identified as an important antecedent of positive attitudes (Jarvenpaa, Tractinsky, & Saarinen, 1999). Similar to the e-commerce context, where a low level of perceived risk, and consequently a lower trust, would prevent consumers from participating in transactions (Hoffman, Novak, & Peralta, 1999), we argue that perceived low risk will be an important factor in the IT decision-making process and consequently, will positively impact the intention to adopt an OSS product. Thus, we hypothesize:

H5c: Lower perceived risk for OSS will have a positive impact on the adoption intention for OSS.

Relationship between Perceived Negative Utility, Perceived Positive Utility, and Adoption Intention

According to the Theory of Reasoned Action, the attitudes of IT decision-makers should generally be a pretty accurate predictor of their individual behavioral intentions (Harrison, Mykytyn Jr, & Riemenschneider, 1997). In this context, we argue that the TRA provides the right theoretical foundation to explain the balance between positive and negative utility. Indeed, we follow the (Benlian & Hess, 2011b) argument that IT decision-maker attitude toward an OSS product is formed by salient behavioral beliefs. More specifically, we hypothesize that the perceived IT security risk, with its four antecedents, will have either a positive or negative effect on IT decision-maker attitude. We posit that an IT decision-maker, during the decision-making process, will 1) review all the perceived IT security-related risks (confidentiality, integrity, availability, and information assurance risks), 2) combine the identified risks, and 3) analyze the impact, benefits, and losses. This process results in positive and negative attitudinal appraisal that will be part of the influential factors impacting an IT decision-maker's adoption intention.

In other contexts (e.g. with Internet services), perceived risk had an important effect on adoption intention (Featherman & Pavlou, 2003). However, it was also shown that perceived risk had a negative effect on the adoption intention in the "business process outsourcing" context (Gewald et al., 2006). Several other studies (e.g. Chwelos, Benbasat, & Dexter, 2001) have confirmed the relationships between the positive and negative utility and perceived risk. Therefore, we do expect to see positive or negative relationships, respectively, between the positive or negative utility in connection to the perceived risk. Thus, we hypothesize:

H6: Perceived negative utility of OSS is negatively associated with the adoption intention for OSS.

H7: Perceived positive utility of OSS is positively associated with the adoption intention for OSS.

4 Research Methodology

In this section, we will explain our research methodology, starting with the surveying instrument.

4.1 Research Setting

A recent survey of the Linux Foundation revealed that Linux (an open source operating system) adoption is experiencing constant growth, especially when it comes to mission-critical applications such as cloud computing, where Linux dominance is very strong (Linux Foundation, 2013). Another survey confirmed that 80% (out of 3,500) of programmers are using open source software in their development lifecycle (Sonatype, 2013). This led us to choose open- source software as our research stimulus, because its importance and growth among enterprise users is high.

4.2 Research Instrument

Our survey instrument was based on an exhaustive literature review and some previous similar studies from other fields, such as e-commerce. Table 1 provides the details of the survey instruments as well as information on the corresponding authors that were used to build the final questionnaires. Also, in order to ensure the highest quality and avoid any possible misunderstandings, we ran a pilot study with seven information security professionals. After receiving their comments and suggestions, we made further adjustments to some of the questions that could have been, according to the pilot study feedback, misleading.

Item	Description

Perceived Lack Of Confidentiality (PC)	I believe Open Source Software may use customer information without permission I believe Open Source Software might alter information in its own self-interest. I believe Open Source Software may lead to potential loss of privacy. Indicators adapted from: (John, 1984)
Perceived Lack Of Integrity (PI)	Information about my Open Source Software activities would be known to others. I believe Open Source Software source code may be modified or deleted by others. I believe there is a high probability of losing information integrity in using Open Source Software. Indicators adapted from: (Bhimani, 1996); (Cockburn & Wilson, 1996); (Sweeney, Soutar, & Johnson, 1999); (Srivastava et al., 2010)
Perceived High Availability (PA)	I believe Open Source Software provides good information availability I believe Open Source Software has a reputation for delivering requested tasks. In general, I believe Open Source Software ensures access to information when needed. Indicators adapted from:(Wu, Li, & Fu, 2011); (Ackermann, Miede, Buxmann, & Steinmetz, 2011); (Ackermann, Widjaja, Benlian, & Buxmann, 2012)
Perceived High Structural Assurance (PSA)	I believe Open Source Software has enough safeguards to be used in organizational activities and tasks. I feel assured that legal and technological structures adequately protect company from problems in Open Source Software. I feel confident that encryption and other technological safeguards make it safe for the company to use Open Source Software. In general, Open Source Software provides robust and safe environment to perform organizational tasks. Indicators adapted from: (McKnight et al., 2002)
Perceived Risk (PR)	I believe Open Source Software is reliable. I believe Open Source Software is secure. I believe Open Source Software is trustworthy. Adopting Open Source Software will not lead to a potential loss. Overall riskiness of Open Source Software is low. Indicators adapted from: (Featherman & Pavlou, 2003); (Nicolaou & McKnight, 2006)
Perceived Negative Utility	Adopting OSS is associated with a high level of risk. There is a high level of risk that the expected benefits of adopting OSS will not

(PNU)	materialize. Overall, I consider the adoption of OSS to be risky. Indicators adapted from: (Featherman & Pavlou, 2003); (Benlian & Hess, 2010)
Perceived Positive Utility (PPU)	Adopting Open Source Software has many advantages. Adopting Open Source Software is a useful instrument for increasing operational excellence. Overall, I consider the adoption of Open Source Software to be a useful strategic option. Indicators adapted from: (Gewald & Dibbern, 2009)
Adoption Intention (AI)	If there is a superior offer, Open Source Software should be used for the application domain I am in charge of. Our company should increase the existing level of adopting Open Source Software. I support the further adoption of Open Source Software. Indicators adapted from: (Gewald & Dibbern, 2009); (Benlian & Hess, 2011a)

Table 1: Items Used for Survey Instrument

The survey ran for two months, from April to May 2014. We addressed (by e-mail) the key informants as follows (in order of preference): the Chief Information Officer (CIO) was our main target that we tried to contact whenever possible. However, in many cases, the CIO function did not exist and only the Chief Executive Officer (CEO) or IT directors were present. Hence, after the CIO we tried to reach any individual serving a similar function (such as a CEO or IT director). Also, in order to make sure that we avoided any eventual data privacy or e-mail spam concerns, we did not send any reminders to the informants. We used an online survey method to contact 850 IT decision-makers from various countries and organizations (400 participants were directly contacted as we had their contact details through previous research studies and 450 participants were contacted through LinkedIn). We did not specifically target users or non-users of OSS products, as we did not want to influence the study results and create a possible bias by selecting only users of OSS technology. However, all contacted participants were involved in the IT decision-making processes and consequently should have had good foundational knowledge to understand the challenges related to perceived IT security risk and OSS. In total, 210 people completed the survey.

The response rate (of 24%) is rather low but is still acceptable with regard to the difficulties in obtaining survey responses from IS executives and corporate-level managers (Poppo & Zenger, 2002). Also, in over

150 cases, we received bounced (not delivered) emails which indicates that many employees do not regularly update their LinkedIn profile. Interestingly, in over 50 cases it seems that LinkedIn profiles are managed by CxO assistants as they replied by confirming that CxO is very busy and may not have time to reply in time.

Finally, we removed 22 responses due to missing data (10) and inconsistent response patterns (12) resulting from implausible short handling times (< 3 minutes). Our final sample accounted for 188 participants.

4.3 PLS Analysis

Our research was built on the survey data, and employs variance-based structural equation modeling (SEM) techniques (Chin, 1998; Chin, Marcolin, & Newsted, 2003). SEM is particularly useful in the IS research where often the key concepts are not directly observable (Roldán & Sánchez-Franco, 2012). Also, it is considered be a "silver bullet" for estimating causal models in many model and data situations (J. Hair, Ringle, & Sarstedt, 2011). The research model was tested using the partial least squares (PLS) approach. Our initial assumption was that all hypothesized relations are linear. Hence, due to the possible non-linear relationships that may be present in our model, standard PLS software packages based on a linear assumption may not be suitable for testing and analyzing our model. We opted for WarpPLS 3.0 (Kock, 2010), a powerful PLS-based structural equation modeling software that has the capability to test both linear and non-linear relationships (e.g. U-shaped and S-shaped functions). Furthermore, covariance-based SEM requires a larger sample size, whereas PLS can produce stable path coefficients and significant p-values with lower sample sizes (usually less than 100) (Kock, 2010).

5 Results

In this section we present our detailed findings. First, we detail the participants demographics. Second, we explore the measurement model results to finish with assessing our initial hypotheses.

5.1 Demographics

In Table 2, participant demographics are detailed.

Country	Nb.	Country	Nb.
Australia	3	Norway	2
Belgium	4	Pakistan	2

Brazil	11	Poland	3
Canada	14	Portugal	1
Chile	2	Romania	1
Croatia	6	Russian Federation	3
Denmark	2	Singapore	2
Finland	2	South Africa	3
France	11	Spain	4
Germany	3	Sweden	2
Greece	3	Switzerland	3
India	6	Taiwan	1
Indonesia	1	Turkey	2
Israel	2	Ukraine	4
Italy	5	United Kingdom	8
Jordan	1	United States	62
Mexico	2	Pakistan	2
Netherlands	7	Poland	3

Table 2: Summary of Respondents by Country

Of the 850 contacted IT decision-makers, we received 188 responses from 34 different countries. Of the 188 participants, 176 were men (93.6%) and 12 were women (6.4%); the average age of the participants was 41.5 years. Table 3 illustrates this distribution.

Age	Number (N)	(%)	Gender	Number (N=188)	(%)
< 30	10	5.3%	Male	176	93.6%
30-40	76	40.4%	Female	8	6.4%
41-50	68	36.1%			
> 50	34	18.2%			

Table 3: Survey Distribution by Age and Gender

Participants originated from various type of industries/organizations: consulting (23.4%), engineering (5.3%), entrepreneurship (2.6%), information technology (32.98%), military and protective services (1.60%), support (1.60%), and other (15.43%). In the other category there were in total 17 different industries represented (i.e. airport, banking, education, finance, government, etc.). When asked about their positions within these organizations, the distribution came out as follows: CIO (74.5%), IT Director (15.4%), Information Security Manager (2.89%), and other (7.21%). There were 18 different positions indicated in the other category (i.e. Architect, Business Systems Security Manager, Developer, Network Admin., etc.). When it comes to professional experience and organizational size, Table 4 shows the participant distribution.

Years of experience	In %	Organization size	In %
1–3 years	53 (28.19%)	Large: over 250 employee	105 (55.85%)
3–8 years	40 (21.27%)	Medium: 50–250 employee	28 (14.89%)
Less than 1 year	25 (13.29%)	Small: less than 50 employee	55 (29.25%)
Over 8 years	70 (37.23%)		

Table 4: Participant Experience and Organization Size

5.2 Measurement Model

To assess the research model fit with the data, the recommended p-values for both the average path coefficient (APC) and the average r-squared (ARS) need to be both lower than 0.05. Additionally, the recommended average variance inflation factor (AVIF) should be lower than 5 (Kock, 2010). In reference to the results from Table 5, both models meet all three criteria, and we have reason to believe that the models have acceptable predictive and explanatory quality.

Model fit indices and P values
APC= 0.359, P<0.001 ARS= 0.546, P<0.001 AVIF= 1.751, Good if < 5

Table 5: Model Fit Indices and p-values

We present the reliability results in Table 6. The composite reliabilities of the different measures range from 0.805 to 0.960, which exceed the recommended threshold value of 0.70. Also, following the recommendation of Fornell and Larcker (1981), the average variance extracted (AVE) for each variable construct exceeds 0.50.

Variable constructs	AVE	Composite Reliability
Perceived Lack of Confidentiality (PC)	0.774	0.911
Perceived Lack of Integrity (PI)	0.673	0.805
Perceived High Availability (PA)	0.826	0.934
Perceived High Structural Assurance (PSA)	0.768	0.930
Perceived Low Risk (PR)	0.795	0.951
Perceived Negative Utility (PNU)	0.783	0.915
Perceived Positive Utility (PPU)	0.888	0.960
Adoption Intention (AI)	0.885	0.959

Table 6: Assessment of the Measurement Model

According to the Fornell-Larcker criterion (Fornell & Larcker, 1981), the AVE of each latent construct should be higher than the construct's highest squared correlation with regard to any other latent construct (Table 6). The discriminant validity test is shown on Table 7, where the square root of the reflective construct's AVE is on the diagonal and the correlations between the constructs are in the lower left triangle. We observe that the discriminant validity test has been established.

	PI	PA	PC	PSA	PR	PNU	PPU	AI
PI	**0.820**							
PA	-0.290	**0.909**						
PC	0.462	-0.382	**0.880**					
PSA	-0.353	0.634	-0.483	**0.876**				
PR	-0.461	0.623	-0.597	0.766	**0.892**			
PNU	0.666	-0.508	0.618	-0.513	-0.661	**0.885**		
PPU	-0.218	0.479	-0.401	0.490	0.594	-0.457	**0.942**	
AI	-0.390	0.610	-0.518	0.653	0.783	-0.629	0.638	**0.941**

Table 7: Discriminant Validity (Intercorrelations) of Variable Constructs

Also, Stone-Geisser Q-squared coefficients were calculated for each of the endogenous variables in the study's path model (Geisser, 1974; Stone, 1974). Endogenous variables with acceptable predictive validity have Q-squared coefficients of greater than zero (Kock, 2010). Each of the endogenous variables in the study's model exhibited Q-squared coefficients greater than zero (PPU 0.364, PNU 0.453, PR 0.702, AI 0.686), thereby presenting acceptable predictive validity.

Furthermore, we performed a full collinearity check that was based on the variance inflation factors (VIFs) for each of the latent variables. VIFs represent the degree of multicollinearity among variables, including both indicators and latent variables (Kock, 2010). Collinearity can be vertical or lateral. Vertical collinearity is a predictor-predictor latent variable collinearity found in individual blocks, while lateral collinearity refers to predictor-criterion latent variable collinearity (Kock, 2010). The recommended VIFs

value should be lower than 5 (J. F. Hair, 2009; Kline, 2011). Considering that the highest VIF score is 4.304 (Table 9), we concluded that no existence of multicollinearity can be supported.

PI	PA	PC	PSA	PR	PNU	PPU	AI
1.878	1.970	1.829	2.716	4.304	2.993	1.809	3.204

Table 8: Full Collinearity VIFs

Simpson's paradox is characterized by the fact that the correlation and path coefficient of a predictor latent variable with respect to a criterion latent variable have opposite signs (Wagner, Torgesen, & Rashotte, 1994). According to Kock (2010), paths that have these opposite signs might be improbable or the direction of the relationship is reversed. In order to address Simpson's paradox in the current model, we examined all links between the predictor and criterion variables. As we did not identify any paths with positive (negative) correlations or negative (positive) path coefficients, we concluded that our model does not contain any instances of a Simpson's paradox.

Using WarpPLS, we checked the cross loadings where discriminant validity is established when an indicator's loading on a construct is higher than all of its cross loadings with other constructs. We present the results in Table 9, which indicates that all the items are more highly loaded on their respective construct than on any other. As shown in Table 9, all but one (PI2) of the items' loadings were greater than 0.70 (all significant, $p < 0.001$). Thus, this item was not retained and was deleted from the model.

	PI	PA	PC	PSA	PR	PNU	PPU	AI
PI1	**0.82**	0.082	0.146	-0.071	-0.155	-0.64	0.056	0.022
PI3	**0.82**	-0.082	-0.146	0.071	0.155	0.64	-0.056	-0.022
PA1	0.044	**0.894**	0.067	0.052	-0.002	-0.047	0.028	0.134
PA2	-0.137	**0.901**	-0.033	-0.048	0.055	0.207	0.016	-0.082
PA3	0.09	**0.932**	-0.032	-0.004	-0.052	-0.155	-0.043	-0.05
PC1	-0.086	0.065	**0.89**	-0.048	0.197	-0.029	0.089	-0.168
PC2	0.096	-0.076	**0.909**	-0.039	0.029	-0.004	0.096	0.026
PC3	-0.013	0.013	**0.839**	0.093	-0.24	0.036	-0.199	0.15
PSA1	0.09	0.062	0.053	**0.886**	0.016	-0.203	-0.099	-0.035
PSA2	-0.112	-0.076	-0.023	**0.869**	0.088	0.279	0.227	-0.196
PSA3	-0.032	-0.097	-0.029	**0.873**	-0.069	0.098	-0.074	0.149
PSA4	0.053	0.108	-0.002	**0.877**	-0.034	-0.169	-0.052	0.082
PR1	0.049	-0.007	0.147	0.027	**0.909**	-0.13	0.031	0.14
PR2	0.084	-0.083	-0.095	0.184	**0.918**	0.034	-0.049	-0.079

PR3	0.07	-0.023	0.038	0.027	**0.952**	-0.159	-0.005	-0.005
PR4	0.041	-0.005	-0.102	0.085	**0.902**	-0.067	0.018	-0.014
PR5	-0.294	0.142	0.012	-0.386	**0.766**	0.39	0.007	-0.05
PNU1	0.336	-0.052	-0.195	0.043	0.004	**0.857**	0.002	0.021
PNU2	-0.137	0.062	0.056	-0.085	0.108	**0.904**	0.05	-0.103
PNU3	-0.184	-0.013	0.131	0.045	-0.113	**0.892**	-0.053	0.084
PPU1	0.012	-0.023	-0.068	0.005	0.036	0.007	**0.936**	-0.004
PPU2	0.041	-0.005	0.013	-0.006	-0.072	-0.095	**0.938**	-0.02
PPU3	-0.052	0.027	0.054	0.001	0.035	0.087	**0.953**	0.024
AI1	0.032	-0.071	0.063	0.047	-0.084	-0.115	0.01	**0.927**
AI2	-0.053	-0.004	-0.04	-0.007	-0.034	0.087	-0.025	**0.953**
AI3	0.022	0.074	-0.022	-0.039	0.117	0.025	0.015	**0.943**

Table 9: Factor Loadings and Cross Loadings

We have now reviewed the initial information by conducting a full collinearity check, doing predictive validity testing (Q-square), looking for the presence of Simpson's paradox instances in the model, and checking factor loadings and cross loadings. We conclude that the initial results indicate that the model findings are meaningful.

5.3 Common Method Bias

As we collected responses from single respondents via the online survey, there is a possibility for common method bias. In an effort to minimize the susceptibility of the study to common methods bias, we provided detailed explanations and examples to all constructs and terms within the survey, which ensured higher realism leading to more responses that are valid. Also, we followed two recommendations as suggested by Philip M. Podsakoff, MacKenzie, Lee, and Podsakoff (2003) to address some specific threats to common method bias: 1) before participants started the survey they had to read a statement that explained that there is no good or bad answer and that their honest answers are expected; and 2) we assured participants that their responses are fully anonymous. Next, we introduced response set questions to be sure that participants would not provide automatic answers without reading questions.

We used two procedures to check for common method variance (CMV): Harman's single-factor test (Philip M. Podsakoff et al., 2003; Philip M Podsakoff & Organ, 1986) and the statistical approach developed by Liang, Saraf, Hu, and Xue (2007). First, we performed Harman's single factor using SPSS software, where all items were entered into an unrotated exploratory factor analysis to check if a single factor accounts for the majority of the variance. Overall, 26 factors emerged (consistent with the

number of constructs in the model), and the largest accounted for 35 percent of the variance. However, Harman's one-factor test is increasingly contested for not being very reliable in detecting comment method bias (Philip M. Podsakoff et al., 2003). Therefore, we used the technique recommended by Liang et al. (2007) which was adapted to PLS from the test suggested by Williams, Edwards, and Vandenberg (2003) and Philip M. Podsakoff et al. (2003). According to Williams et al. (2003), evidence of common method bias can be obtained by examining the statistical significance of factor loadings of the method factor and comparing the variances of each observed indicator explained by its substantive construct and the method factor. Hence, the method suggests that the squared values of the method factor loadings should be interpreted as the percent of indicator variance caused by method. Also, the squared loadings of substantive constructs should be interpreted as the percent of indicator variance caused by substantive constructs. We created a single-indicator factor for each indicator in the measurement model. Further, all independent constructs are linked to the single-indicator constructs. Then, we introduced the "common method factor" whose indicators included all the principal constructs' indicators.

The average substantively explained variance of the indicators is 0.802, while the average variance explained by the method factor is 0.008. The ratio of substantive construct variance to common method variance is about 106:1. Finally, as our study reflects a very small influence due to common method bias, we conclude that common method bias is not a concern for this research.

5.4 Structural Model

To assess our hypotheses, we examined the parameters provided by the PSL structural model. We applied the bootstrapping resampling procedure (500 samples) to estimate the significance of paths in our structural model. Also, R^2 values of the dependent variables represent the predictability of the theoretical model and standardized path coefficients indicate the strength of the relationship between the independent and dependent variable (Chin, 1998). To assess our hypotheses, we examined the parameters provided by the PSL structural model. The results are shown in Figure 3.

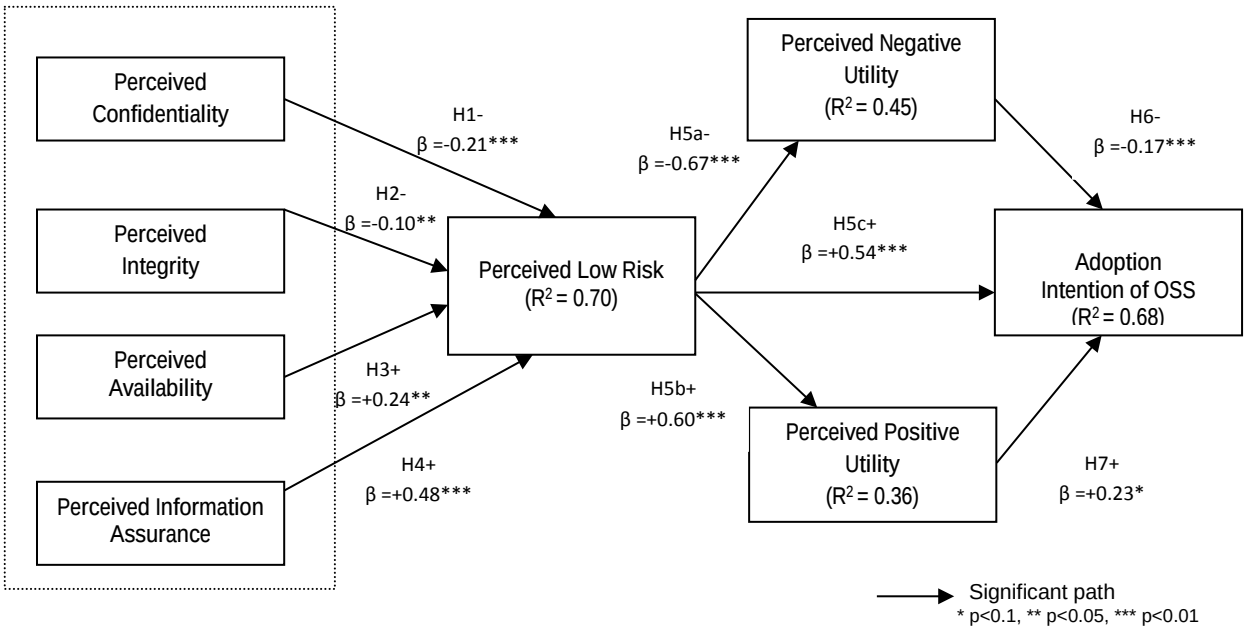

Figure 3. Structural Model Results

The results indicate an R^2 value of 0.68, which means that the theoretical model explained a substantial amount of variance in the adoption intention. Also, the model accounts for 70% of the variance for perceived risk in OSS. Taking into account the 10% criterion, which suggests that the R^2 value of a dependent variable should be at least 10% in order to make a meaningful interpretation, our theoretical model shows substantial explanatory power. Hence, the R^2 value of 0.68 indicates that the theoretical model explained a substantial amount of variance in *adoption intention* for OSS.

Our structural model results indicate that all of our hypotheses are supported. Perceived lack of confidentiality (β = -0.21, $p < 0.01$), perceived lack of integrity (β = -0.10, $p < 0.05$), perceived high availability (β = +0.24, $p < 0.05$), and perceived high structural assurance (β = +0.48, $p < 0.01$) had significant effects on perceived risk, thereby supporting hypotheses 1, 2, 3, and 4. In addition, perceived risk (β = -0.67, $p < 0.01$) had a significant effect on the perceived negative utility. Also, perceived risk (β = +0.60, $p < 0.01$) positively impacted the perceived positive utility and perceived risk (β = +0.54, $p < 0.01$) had significant effects on the adoption intention. Finally, perceived negative utility (β = -0.17, $p < 0.01$) and perceived positive utility (β = +0.23, $p < 0.01$) had significant effects on the adoption intention. Hence, hypotheses H5a, H5b, H5c, H6, and H7 were supported.

5.5 Structural Model without PNU and PPU

We also wanted to understand the relation between the perceived IT security risk and adoption intention (i.e. to assess the theory without the PNU and PPU.. Hence, we removed the perceived positive and perceived negative utility constructs from our model. The structural model is shown on Figure 4.

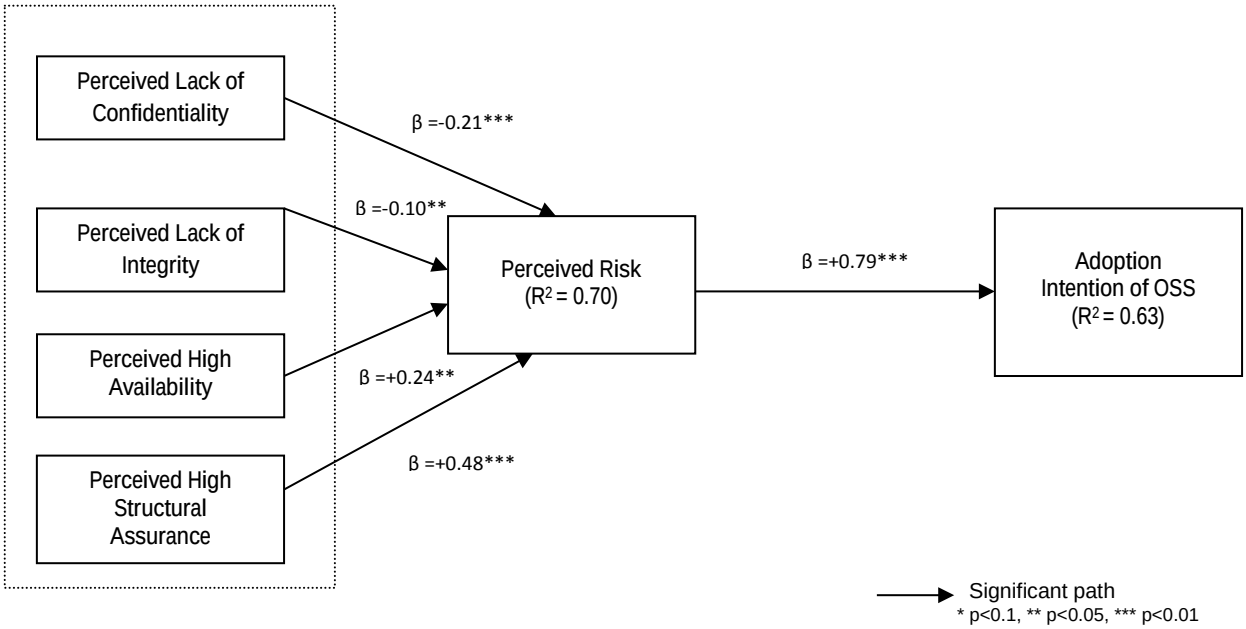

Figure 4: Structural Model Results without PNU/PPU

The structural model indicates that the perceived risk (β = +0.79, p < 0.01) had a significant effect on the adoption intention. The R^2 value of 0.63 indicates that the theoretical model explained a substantial amount of variance in the *adoption intention* of OSS. Hence, there is a strong positive relationship between the perceived IT security risk and adoption intention.

6 Discussion

This research aimed at answering the question if OSS characteristics affect the risk perception and OS IT decision-making process. Our research reveals important antecedents to the perceived IT security risks of: confidentiality, integrity, availability, and information assurance.

Perceived low integrity and perceived low confidentiality have significant negative relationships with the perceived IT security risk of OSS. This is in line with past literature (Pavlou, Huigang, & Yajiong, 2007a). Our results suggest that perceived low integrity and perceived low confidentiality are important factors

influencing perceived IT security risk. Both dimensions seem to be very important for an IT decision-maker's risk-related behaviors. Indeed this "opportunistic OSS behavior" can be labeled as data privacy and compliance issues, to which enterprises are very sensitive today. It is clear that the risk behind the use of OSS and the fact that by its nature, OSS source code can be accessed and modified by unknown individuals, directly influences the IT decision-maker. Thompson (1984), in his "Reflections on trusting trust," an awarded paper, highlighted how modifying the original source code of the C language compiler (C is a general-purpose computer programming language) can produce a dangerous program. His work raised an important question about trusting the trust. Indeed, OSS from its inception down to its use within organizations can go through various adaptations, and as such, trust becomes a critical element to consider and understand. This confirms that "loss of privacy" is one of the most important concerns related to the adoption of a new product where information protection is highly important (Featherman & Pavlou, 2003; Kim et al., 2008).

Availability is an important antecedent to the perceived IT security risk. For enterprises, this suggests that access to data and services is of highest importance. OSS is considered to be reliable and thus, has a good reputation in providing the requested services when needed. We found that perceived availability positively influences the perceived IT security risk. We argue that reliability coincides with reputation, which, in turn, brings trust to an OSS product. This is in line with McKnight et al. (2002)'s argument: "Trust in technology is built the same way as trust in people. When users first experience technology, signals of well-done user interfaces and good vendor reputations will build trust. Reliable, dependable, quality IT performance is the key over time . . . the entire system infrastructure should demonstrate quality." Several past studies, in other contexts, confirmed that when system or service availability is adequately provided, the perceived risk will decrease (Pavlou et al., 2007b). Hence, availability is a very important antecedent to the perceived IT security risk that should be carefully examined and taken into consideration by an IT decision-maker.

As expected, empirical results confirmed our hypotheses of the perceived structural assurance having a strong positive influence on the perceived IT security risk. The higher the perceived structural assurance (i.e. technological safeguards, legal and technological structures, and encryption risk) the more likely there will be a trustworthy relationship. It is clear that an IT decision-maker will be guided by this positive assurance of information safety and the corresponding technological safeguards. This finding is consistent with previous risk-related findings (e.g. Grazioli & Jarvenpaa, 2000; Malhotra, Kim, & Agarwal,

2004; Pavlou, 2003). Interestingly, perceived structural assurance has the strongest relationship with perceived risk among all four theorized antecedents of perceived risk.

It was already found that OSS technology has an important dual-use, where OSS can be used for positive or negative aims (Silic, 2013). If introduced in the organizational ecosystem, its intentions may not always be honest and fair, since organizations rely on the programming results of mostly anonymous strangers in cyberspace, where the issue of trust is omnipresent (De Laat, 2010). We found that perceived positive utility and perceived negative utility have positive and negative significant influences, respectively, on the intention to adopt OSS. This is an important finding as it shows that the five dimensions of the perceived IT security risk play a significant role in defining and shaping the potential benefits (positive utility) or losses (negative utility). Hence, IT decision-maker opinion may be influenced by the perceived benefits or losses where, interestingly, the perceived positive utility of an OSS product has a stronger influence on an IT decision-maker than the positive negative utility. This is in line with past studies where perceived opportunities and benefits had higher influence on adoption intention compared to perceived risk (e.g. Benlian & Hess, 2011a). In order to achieve high information assurance, building institution-based trust could be the right direction. This institutional trust would act as the protector and provider of the much needed safeguards, such as data encryption or application authentication measures. As a result, information, privacy, and possible financial losses can be prevented or reduced to a minimum (McKnight et al., 2002). Moreover, any other legal or compliance structures and safeguards can help to reduce IT security risk in the OSS context. Confidence in the technological safeguards of OSS technology could be another factor reducing the perceived risk.

Our study has another important finding. We identified a strong positive relationship between the perceived IT security risk and adoption intention. Certainly there are other factors that influence adoption intentions, such as subjective norm (Ajzen & Fishbein, 1980), perceived benefits (Chwelos et al., 2001), and economic and strategic risks (Benlian & Hess, 2011b); however, our study found that the perceived IT security risk explains 63% of the dependent variable's variance. This shows the importance of the risk-related factors and the perceived risk dimension's relation to the OSS adoption intention.

Finally, our results are consistent with the Theory of Reasoned Action, and do confirm that the attitudes of IT decision-makers are a good predictor of their individual behavioral intentions (Harrison et al., 1997). More specifically, our results showed how the balance between the positive and negative utility is dependent on the perceived IT security risk, where IT decision-maker attitude toward an OSS product is formed by salient behavioral beliefs.

6.1 Theoretical Contributions

Our research offers several significant and novel contributions to the Information Systems security literature. Firstly, in the existing IS security literature, the relationships between IT security risk, its antecedents, and adoption intention have not been adequately addressed. We aimed to fill this gap by explaining this complex relationship in depth and providing novel insights on the IT security risk antecedents: perceived low confidentiality, perceived low integrity, perceived high availability, and perceived high structural assurance. Our research offers theoretical understandings of the complex interplay between the IT decision-making factors and the process related to OSS adoption. To the best of our knowledge, this research represents the first empirical study that investigates the perceived IT security risk relationship with adoption intention in the OSS context. More specifically, we suggest several new theoretical insights that will help to better scope, understand, and clarify the perceived risk-related antecedents and their influence on OSS product adoption.

Secondly, future research can use our research findings as the starting point to better understand the OSS adoption context and the importance of perceived risk and its direct and significant relationship with adoption intention. In addition, the study revealed four novel risk-related antecedents that should be further analyzed and better understood. We believe IS security research demands more research on risk-related topics, especially in the context of the mobile world, where the importance of the "risk in mobile apps" topic is very significant and calls for more research.

Thirdly, our research established the greater significance of perceived positive utility over perceived negative utility. While past studies have established the same relationships in other contexts, this is an important theoretical contribution since it could explain the current open source software usage growth among enterprises. However, this would need to be further proved and investigated to better understand the phenomenon.

Fourthly, the four theorized antecedents of the perceived IT security risk explain a significantly high percentage of variance in perceived risk. In the context of OSS adoption, the presented antecedents of the perceived risk extend the existing risk literature on OSS adoption. We have also provided a solid framework, proposing theoretical foundations to better understand the relationship between perceived risk and its antecedents.

Finally, our study highlighted the importance of perceived risk on the adoption intention, where perceived risk alone has a strong influence on the adoption intention and is consequently an important factor in the IT decision-making process.

6.2 Practical Implications

Our study offers several implications for practitioners. Better understanding the perceived risk antecedents and the relationship with the adoption intention can clearly facilitate the IT decision-making process. Our research found a strong relationship between perceived risk and OSS adoption intention. In this context, having strong confidentiality and integrity, where data privacy and integrity will be safe and protected, would bring more trust and consequently, would reduce potential risks in OSS. Moreover, strong technological safeguards, the availability of the data, and service (e.g. Linux server or cloud solutions) when it is requested and needed, are the keys to achieving a trustworthy relationship between an IT decision-maker and an OSS product. In this context, risk seems to be a highly important driver facilitating the decision-making process. These four risk antecedents should be taken as important factors to take into account when adopting a new OSS product. The overall acceptance of an OSS product may depend very much on the risk-related antecedents and as such, they require more focus from decision-makers.

Finally, we argue that not only the users (enterprises) of the OSS products should review all the risk-related antecedents when considering OSS product adoption, but also the makers themselves (i.e. developers). More precisely, OSS makers should reflect on their programming practices and adapt them to any new and different needs. Indeed, the example of the Heartbleed bug (Riley, 2014) showed an inconsistency in the way OSS products are tested and verified for bugs. Thus, this research could also be beneficial for OSS programmers since it shows that more formal tests are needed in order to ensure OSS quality—but more than anything, emphasis should be placed on this matter to ensure a trustworthy relationship with IT decision-makers. OSS developers will need to implement better tests, checks, and verifications of OSS code. By doing this, they will help reduce the overall perceived risks related to OSS and will minimize the challenge behind “trusting the trust.”

6.3 Limitations and Future Research

Our study has several limitations. Firstly, it was very difficult to distinguish enterprises that are users of OSS from non-users, as today, OSS is present at different layers of the organizational ecosystem. This could have some influence on our results since performing any sub-group analysis could be biased by

this limitation. Secondly, we did not limit the scope of OSS to certain OSS categories or types. The study results would probably be more precise if we selected certain OSS type (for instance, limiting the survey to only desktop OSS, such as Linux). In this case, the separation of the users from the non-users would be easier and the results would be more precise. Thirdly, we used theory of reasoned action (TRA) to theoretically support our study, which could be seen as a limiting factor as TRA is a model addressing individual behavior. However, we believe TRA is appropriate to be used as not only TRA was used in several past studies to understand organizational decision-making behavior through individual behavior, but also individual behavior is often driving the entire organizational behavior.

We suggest that future research try to focus more on precise OSS types, such as the Linux operating system, in an enterprise context to better understand how risk influences adoption intention. For example, it would be interesting to do a longitudinal study of a type of OSS (e.g. Linux) and examine the regional cultural dimension such as comparing North America (USA and Canada) with Europe or comparing Asia with the rest of the first world (i.e. Europe and North America). Another direction would be to introduce the cultural aspect by introducing cultural dimension antecedents, because it could be interesting to understand how cultural context influences the IT decision-making OSS adoption process. Finally, future studies could investigate the importance of the "trusting the trust" dimension and how it relates to the adoption intention with regard to OSS.

7 Conclusion

Our research investigated the risk factors that influence the IT decision-making process with regard to OSS adoption by using theory of reasoned action. The study offers novel insights on the importance of perceived risk in OSS adoption intention. We provide new theoretical contributions to the existing literature and extend the current understanding of risk-related factors. Furthermore, we identified four important antecedents (confidentiality, integrity, availability, and information assurance) for IT security risk that can used in future studies as an initial theoretical foundation. Finally, we believe that this study provides important insights for information professionals in their decision-making process during the adoption of a new OSS product. Also, it shows the strategic path to take for OSS developers who need to adapt their programming mindset if they want to establish a higher trustworthy relationship. At the end, this paper contributes to the existing openness phenomenon, where risk is more visible, tangible and highlighted by OSS opponents and mass media.

8 References

Ackermann, T., Miede, A., Buxmann, P., & Steinmetz, R. (2011). *Taxonomy of technological IT outsourcing risks: support for risk identification and quantification.* Paper presented at the ECIS.

Ackermann, T., Widjaja, T., Benlian, A., & Buxmann, P. (2012). Perceived IT security risks of cloud computing: Conceptualization and scale development.

Ågerfalk, P. J., Deverell, A., Fitzgerald, B., & Morgan, L. (2005). *Assessing the role of open source software in the European secondary software sector: a voice from industry.* Paper presented at the Proceedings of the 1st International Conference on Open Source Systems (Scotto, M. and Succi, G. Eds.).

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour.

Aldridge, A., White, M., & Forcht, K. (1997). Security considerations of doing business via the Internet: cautions to be considered. *Internet Research, 7*(1), 9-15.

Alhazmi, O. H., Malaiya, Y. K., & Ray, I. (2007). Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers & Security, 26*(3), 219-228. doi: 10.1016/j.cose.2006.10.002

Amoroso, E. G. (1994). *Fundamentals of computer security technology*: Prentice-Hall, Inc.

Benlian, A., & Hess, T. (2010). *The Risks of Sourcing Software as a Service-An Empirical Analysis of Adopters and Non-Adopters.* Paper presented at the ECIS.

Benlian, A., & Hess, T. (2011a). Comparing the relative importance of evaluation criteria in proprietary and open-source enterprise application software selection - a conjoint study of ERP and Office systems. [Article]. *Information Systems Journal, 21*(6), 503-525. doi: 10.1111/j.1365-2575.2010.00357.x

Benlian, A., & Hess, T. (2011b). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems, 52*(1), 232-246.

Bettman, J. R. (1973). Perceived Risk and Its Components: A Model and Empirical Test. *Journal of Marketing Research (JMR), 10*(2).

Bhimani, A. (1996). Securing the commercial Internet. *Communications of the ACM, 39*(6), 29-35.

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management.* Paper presented at the Proceedings of the 2001 workshop on New security paradigms.

Boehm, B. W. (1981). Software engineering economics.

Bonaccorsi, A., & Rossi, C. (2003). Why open source software can succeed. *Research Policy, 32*(7), 1243-1258. doi: 10.1016/s0048-7333(03)00051-9

Bozeman, B., & Kingsley, G. (1998). Risk culture in public and private organizations. *Public Administration Review*, 109-118.

Browne, H. K., Arbaugh, W. A., McHugh, J., & Fithen, W. L. (2001). *A trend analysis of exploitations.* Paper presented at the Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on.

Carter, L., & Belanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5-25. doi: 10.1111/j.1365-2575.2005.00183.x

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295*(2), 295-336.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information systems research, 14*(2), 189-217.

Chou, S. W., & He, M. Y. (2011). Understanding OSS development in communities: the perspectives of ideology and knowledge sharing. *Behaviour & Information Technology, 30*(3), 325-337. doi: 10.1080/0144929x.2010.535853

Chwelos, P., Benbasat, I., & Dexter, A. S. (2001). Research report: empirical test of an EDI adoption model. *Information systems research, 12*(3), 304-321.

CNBC. (2013). Apple moves to take care of business users Retrieved December 2014, from http://www.cnbc.com/id/101190135/page/1

Cockburn, C., & Wilson, T. D. (1996). Business use of the world-wide web. *International Journal of Information Management, 16*(2), 83-102.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *Journal of applied psychology, 92*(4), 909.

Cowan, C. (2003). Software security for open-source systems. *Security & Privacy, IEEE, 1*(1), 38-45. doi: 10.1109/msecp.2003.1176994

Culp, C. L. (2002). *The risk management process: Business strategy and tactics* (Vol. 103). New York, NY: John Wiley & Sons.

Cunningham, S. M. (1967). The major dimensions of perceived risk. *Risk taking and information handling in consumer behavior*, 82-108.

De Laat, P. B. (2010). How can contributors to open-source communities be trusted? On the assumption, inference, and substitution of trust. *Ethics and Information Technology, 12*(4), 327-341.

Dedrick, J., & West, J. (2003). *Why firms adopt open source platforms: a grounded theory of innovation and standards adoption.* Paper presented at the Proceedings of the workshop on standard making: A critical research frontier for information systems.

Del Bianco, V., Lavazza, L., Morasca, S., & Taibi, D. (2011). A survey on open source software trustworthiness. *Software, IEEE, 28*(5), 67-75.

Deloitte. (2012). Open mobile survey Retrieved September 2014, from http://www.deloitte.com/assets/Dcom-Turkey/Local%20Assets/Documents/turkey_tr_tmt_openmobile_220212.pdf

Dionne, G. (2013). Risk Management: History, Definition, and Critique. *Risk Management and Insurance Review, 16*(2), 147-166.

Eryilmaz, E., Cochran, M., & Kasemvilas, S. (2009, 5-8 Jan. 2009). *Establishing Trust Management in an Open Source Collaborative Information Repository: An Emergency Response Information System Case Study.* Paper presented at the System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on.

Faisst, U., & Prokein, O. (2005). *An optimization model for the management of security risks in banking companies.* Paper presented at the E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on.

Fang, X. W., Chan, S., Brzezinski, J., & Xu, S. (2005). Moderating effects of task type on wireless technology acceptance. *Journal of Management Information Systems, 22*(3), 123-157.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International journal of human-computer studies, 59*(4), 451-474.

Featherman, M. S., Valacich, J. S., & Wells, J. D. (2006). Is that authentic or artificial? Understanding consumer perceptions of risk in e-service encounters. *Information Systems Journal, 16*(2), 107-134.

Federspiel, S. B., & Brincker, B. (2010). Software as Risk: Introduction of Open Standards in the Danish Public Sector. *Information Society, 26*(1), 38-47. doi: 10.1080/01972240903423345

Fichman, R. G. (2000). The diffusion and assimilation of information technology innovations. *Framing the domains of IT management: Projecting the future through the past*, 105-127.

Fischhoff, B. (1995). Risk perception and communication unplugged: Twenty years of process1. *Risk Analysis, 15*(2), 137-145.

Fitzgerald, B., & Kenny, T. (2004). Developing an information systems infrastructure with open source software. *Software, IEEE, 21*(1), 50-55.

Forge, S. (2006). The rain forest and the rock garden: the economic impacts of open source software. *info, 8*(3), 12-31.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research (JMR), 18*(1).

Forrester. (2004). The Costs and Risks of Open Source Retrieved December 2014, from www.forrester.com/Research/Document/0,7211,34146,00.html

Franch, X., Susi, A., Annosi, M. C., Ayala, C., Glott, R., Gross, D., . . . Thomas, C. (2013). *Managing Risk in Open Source Software Adoption.* Paper presented at the Proc. 8th Int. Conf. on Software Engineering and Applications (ICSOFT-EA 2013). SciTePress.

Frei, S., May, M., Fiedler, U., & Plattner, B. (2006). *Large-scale vulnerability analysis.* Paper presented at the Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense.

Garfield, M. J., & McKeown, P. G. (1997). Planning for Internet security. *Information Systems Management, 14*(1), 41-46.

Gartner. (2011). Critical Strategies to Manage Risk and Maximize Business Value of Open Source in the Enterprise Retrieved December 2014, from https://www.gartner.com/doc/1730521/critical-strategies-manage-risk-maximize

Gartner. (2014). Road Map for Open-Source Success Understanding Quality and Security Retrieved December 2014, 2014, from https://www.gartner.com/doc/2674615/road-map-opensource-success-understanding

Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika, 61*(1), 101-107.

Germonprez, M., Young, B., Mathiassen, L., Kendall, J. E., Kendall, K. E., & Warner, B. (2012). Risk Mitigation in Corporate Participation with Open Source Communities: Protection and Compliance in an Open Source Supply Chain.

Gewald, H., & Dibbern, J. (2005). The influential role of perceived risks versus perceived benefits in the acceptance of business process outsourcing: empirical evidence from the German Banking Industry. *E-Finance Lab Working Paper, 9*.

Gewald, H., & Dibbern, J. (2009). Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. *Information & Management, 46*(4), 249-257.

Gewald, H., Wüllenweber, K., & Weitzel, T. (2006). The influence of perceived risks on banking managers' intention to outsource business processes-a study of the German banking and finance industry. *Journal of electronic commerce research, 7*(2).

Goode, S. (2005). Something for nothing: management rejection of open source software in Australia's top firms. *Information & Management, 42*(5), 669-681.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 30*(4), 395-410.

Gregory, R., & Mendelsohn, R. (1993). Perceived risk, dread, and benefits. *Risk Analysis, 13*(3), 259-264.

Guth. (2006). Limiting factors for the adoption of open source software.

Hair, J., Ringle, C., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *The Journal of Marketing Theory and Practice, 19*(2), 139-152.

Hair, J. F. (2009). *Multivariate data analysis*. Upper Saddle River: Prentice Hall.

Harrington, S. E., & Niehaus, G. R. (1999). *Risk management and insurance*. Danvers: Wiley.

Harrison, D. A., Mykytyn Jr, P. P., & Riemenschneider, C. K. (1997). Executive decisions about adoption of information technology in small business: Theory and empirical tests. *Information systems research, 8*(2), 171-195.

Hauge, Ø., Ayala, C., & Conradi, R. (2010). Adoption of open source software in software-intensive organizations–A systematic literature review. *Information and Software Technology, 52*(11), 1133-1154.

Herbsleb, J. (2002). Research Priorities in Open Source Software Development Retrieved December 2014, from http://www.flossproject.org/workshop/papers/herbsleb.htm

Hill, C. W. (1990). Cooperation, opportunism, and the invisible hand: Implications for transaction cost theory. *Academy of Management Review, 15*(3), 500-513.

Hissam, S. A., Plakosh, D., & Weinstock, C. (2002). Trust and vulnerability in open source software. *IEE Proceedings - Software, 149*(1), 47. doi: 10.1049/ip-sen:20020208

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80-85.

Hubspan. (2011). Hubspan-User-Environment-Survey-Final-Results-2011.

IDC. (2004). End-User Perspectives on Cost, Substitutability, Trustworthiness, Support and Adoption: Industry Report

Infrastructure, P. K., & Profile, T. P. (2002). Common criteria for information technology security evaluation. *National Security Agency* Retrieved December 2014, from http://www.dtic.mil/dtic/tr/fulltext/u2/a406677.pdf

ISO. (2008). Information technology -- Security techniques-Information security risk management Retrieved December 2014, from http://www.iso.org/iso/catalogue_detail?csnumber=56742

Jaaksi, A. (2007). Experiences on product development with open source software *Open source development, adoption and innovation* (pp. 85-96). Limerick, Ireland: Springer.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), 0-0.

John, G. (1984). An empirical investigation of some antecedents of opportunism in a marketing channel. *Journal of marketing Research*, 278-289.

Kenwood, C. A. (2001). A business case study of open source software Retrieved December 2014, from http://www.dtic.mil/dtic/tr/fulltext/u2/a459563.pdf

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564.

Kline, R. B. (2011). *Principles and practice of structural equation modeling*. New York, NY: Guilford press.

Kock, N. (2010). *WarpPLS 4.0 User Manual*. Laredo Texas USA: ScriptWarp Systems.

Koller, M. (1988). Risk as a determinant of trust. *Basic and Applied Social Psychology, 9*(4), 265-276.

Kou, G., Peng, Y., Shi, Y., & Wu, W. (2012). Classifier Evaluation for Software Defect Prediction. *Studies in Informatics and Control, 21*(2), 118.

Kou, G., Peng, Y., & Wang, G. (2014). Evaluation of clustering algorithms for financial risk analysis using MCDM methods. *Information Sciences, 275*, 1-12.

Kou, G., Shi, Y., & Dong, G. (2012). Data mining for software trustworthiness. *Information Sciences, 191*, 1-2.

Krishnamurthy, S. (2003). A managerial overview of open source software. *Business Horizons, 46*(5), 47-56.

Kwon, T. H., & Zmud, R. W. (1987). *Unifying the fragmented models of information systems implementation.* Paper presented at the Critical issues in information systems research.

Laplante, P., Gold, A., & Costello, T. (2007). Open Source Software: Is It Worth Converting? *IT Professional, 9*(4), 28-33. doi: 10.1109/mitp.2007.72

Li, Y., Tan, C.-H., & Yang, X. (2013). It is all about what we have: A discriminant analysis of organizations' decision to adopt open source software. *Decision Support Systems, 56*, 56-62.
Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS quarterly, 31*(1), 59-87.
Linux Foundation. (2013). 2013 Enterprise End User Report.
Macredie, R. D., & Mijinyawa, K. (2011). A theory-grounded framework of Open Source Software adoption in SMEs. *European Journal of Information Systems, 20*(2), 237-250.
Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin, 18*(1), 3-9.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information systems research, 15*(4), 336-355.
McGhee, D. D. (2007). Free and open source software licenses: benefits, risks, and steps toward ensuring compliance. *Intellectual Property & Technology Law Journal, 19*(11), 5.
McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: an integrative typology. *Information systems research, 13*(3), 334-359.
Morgan, L., & Finnegan, P. (2007a). Benefits and drawbacks of open source software: an exploratory study of secondary software firms *Open Source Development, Adoption and Innovation* (pp. 307-312): Springer.
Morgan, L., & Finnegan, P. (2007b). *How perceptions of open source software influence adoption: An exploratory study.* Paper presented at the Proceedings of the 15th European Conference on Information Systems (ECIS 2007).
Nagy, D., Yassin, A. M., & Bhattacherjee, A. (2010). Organizational adoption of open source software: barriers and remedies. *Communications of the ACM, 53*(3), 148-151.
Netcraft. (2014). Web server survey Retrieved January 2015, from http://news.netcraft.com/archives/2013/08/09/august-2013-web-server-survey.html
Neuhaus, S., Zimmermann, T., Holler, C., & Zeller, A. (2007). *Predicting vulnerable software components.* Paper presented at the Proceedings of the 14th ACM conference on Computer and communications security.
Nicolaou, A. I., & McKnight, D. H. (2006). Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. *Information systems research, 17*(4), 332-351.
Pavlou. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International journal of electronic commerce, 7*(3), 101-134.
Pavlou, Huigang, & Yajiong. (2007a). Understanding and mitigating uncertainty in online environments: a principal-agent perspective. [Article]. *MIS quarterly, 31*(1), 105-136.
Pavlou, Huigang, & Yajiong. (2007b). UNDERSTANDING AND MITIGATING UNCERTAINTY IN ONLINE EXCHANGE RELATIONSHIPS: A PRINCIPAL--AGENT PERSPECTIVE. [Article]. *MIS Quarterly, 31*(1), 105-136.
Payne, C. (2002). On the security of open source software. *Information Systems Journal, 12*(1), 61-78. doi: 10.1046/j.1365-2575.2002.00118.x
PC World. (2014). Is open source to blame for the Heartbleed bug? Retrieved May 2015, from http://www.pcworld.com/article/2141740/is-open-source-to-blame-for-the-heartbleed-bug.html
Peng, Y., Kou, G., Wang, G., Wang, H., & Ko, F. I. (2009). Empirical evaluation of classifiers for software risk management. *International Journal of Information Technology & Decision Making, 8*(04), 749-767.
Perens, B. (1999). The open source definition *Open sources: voices from the open source revolution* (pp. 171-185). New York, NY: Google.

Peter, J. P., & Tarpey Sr, L. X. (1975). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research*, 29-37.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology, 88*(5), 879.
Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of management, 12*(4), 531-544.
Poppo, L., & Zenger, T. (2002). Do formal contracts and relational governance function as substitutes or complements? *Strategic management journal, 23*(8), 707-725.
Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage: Harvard Business Review, Reprint Service.
Pressman, R. S., & Jawadekar, W. S. (1987). Software engineering. *New York 1992*.
Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. *Risk Analysis, 30*(6), 881-886.
Ratnasingham, P. (1998). EDI security: The influences of trust on EDI risks. *Computers & Security, 17*(4), 313-324. doi: 10.1016/s0167-4048(98)80012-6
Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security, 31*(2), 221-232.
Riley, M. (2014). Nsa said to exploit heartbleed bug for intelligence for years. *Bloomberg News, April, 12*.
Roldán, J. L., & Sánchez-Franco, M. J. (2012). Variance-Based Structural Equation Modeling: Guidelines for Using Partial Least Squares. *Research methodologies, innovations and philosophies in software systems engineering and information systems*, 193.
Rudzki, J., Kiviluoma, K., Poikonen, T., & Hammouda, I. (2009, 27-29 Aug. 2009). *Evaluating Quality of Open Source Components for Reuse-Intensive Commercial Solutions.* Paper presented at the Software Engineering and Advanced Applications, 2009. SEAA '09. 35th Euromicro Conference on.
Sans. (2009). Security Concerns in Using Open Source Software for Enterprise Requirements Retrieved January 2015, from http://www.sans.org/reading-room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements-1305
Scacchi, W. (2007). *Free/open source software development.* Paper presented at the Proceedings of the the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering.
Schryen. (2009). Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities. *AMCIS 2009 Proceedings*.
Schryen. (2011). Is Open Source Security a Myth? [Article]. *Communications of the ACM, 54*(5), 130-140. doi: 10.1145/1941487.1941516
Schweik, C. M., & English, R. C. (2012). *Internet success: a study of open-source software commons*: MIT Press.
Shaikh, M., & Cornford, T. (2012). Strategic Drivers of Open Source Software Adoption in the Public Sector: Challenges and Opportunities. *ECIS 2012 Proceedings*.
Silic, M. (2013). Dual-use open source security software in organizations – Dilemma: Help or hinder? *Computers & Security, 39, Part B*(0), 386-395. doi: http://dx.doi.org/10.1016/j.cose.2013.09.003
Sonatype. (2013). Sonatype Survey Findings Retrieved January 2015, from http://img.en25.com/Web/SonatypeInc/%7B43071d5d-4e57-4fa7-9663-cf967945be95%7D_Sonatype_2013Survey.pdf
Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS quarterly, 34*(3).

Srivastava, S. C., Chandra, S., & Theng, Y.-L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems, 27*, 561-588.

Stewart, K., & Gosain, S. (2001). An Exploratory Study of Ideology and Trust in Open Source Development Groups. *ICIS 2001 Proceedings*.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society. Series B (Methodological)*, 111-147.

Strategyanalytics. (2013). Global Smartphone OS Market Share by Region Q3 2013 Retrieved February 2015, from http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=9095

Sun, L. L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems, 22*(4), 109-142. doi: 10.2753/mis0742-1222220405

Sweeney, J. C., Soutar, G. N., & Johnson, L. W. (1999). The role of perceived risk in the quality-value relationship: a study in a retail environment. *Journal of retailing, 75*(1), 77-105.

The Register. (2013). Ruby off the Rails: Enormo security hole puts 240k sites at risk Retrieved February 2015, from http://www.theregister.co.uk/2013/01/10/ruby_on_rails_security_vuln/

Thompson, K. (1984). Reflections on trusting trust. *Communications of the ACM, 27*(8), 761-763.

Tiangco, F., Stockwell, A., Sapsford, J., Rainer, A., & Swanton, E. (2005). Open-source software in an occupational health application: the case of Heales Medical Ltd. *Procs*.

Vacca, J. R. (2012). *Computer and information security handbook*: Newnes.

van Rooij, S. W. (2007). Perceptions of Open Source versus Commercial Software: Is Higher Education Still on the Fence? *Journal of Research on Technology in Education, 39*(4), 433-453.

Varian, H. R., & Shapiro, C. (2003). Linux adoption in the public sector: An economic analysis. *Manuscript. University of California, Berkeley*.

Ven, K., & Verelst, J. (2012). A Qualitative Study on the Organizational Adoption of Open Source Server Software. *Information Systems Management, 29*(3), 170-187.

Ven, K., Verelst, J., & Mannaert, H. (2008). Should you adopt open source software? *Software, IEEE, 25*(3), 54-59.

Wagner, R. K., Torgesen, J. K., & Rashotte, C. A. (1994). Development of reading-related phonological processing abilities: New evidence of bidirectional causality from a latent variable longitudinal study. *Developmental psychology, 30*(1), 73.

Wheeler, E., & Swick, K. (2011). *Security risk management: building an information security risk management program from the ground up*: Syngress.

Whitman, M., & Mattord, H. (2013). *Management of information security*: Cengage Learning.

Williams, L. J., Edwards, J. R., & Vandenberg, R. J. (2003). Recent advances in causal modeling methods for organizational and management research. *Journal of management, 29*(6), 903-936.

Williamson, O. E. (1975). Markets and hierarchies. *New York*, 26-30.

Wolke, T. (2008). *Risikomanagement*: Oldenbourg Verlag.

Wu, L., Li, J.-Y., & Fu, C.-Y. (2011). The adoption of mobile healthcare by hospital's professionals: An integrative perspective. *Decision Support Systems, 51*(3), 587-596.

Yue, W. T., Çakanyıldırım, M., Ryu, Y. U., & Liu, D. (2007). Network externalities, layered protection and IT security risk management. *Decision Support Systems, 44*(1), 1-16.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583-592.