Risk Management Governance in Applications

Rasha Mohammed Alolayan
Information System Department, College of Computer and Information Sciences KSA (2020)

Abstract
This paper is an overview of risk management governance in applications, a detailed discussion has been provided regarding the importance of developing and implementing a well-organized risk management governance that will enhance the trust of the users when it comes to using an application and at the same time will also provide them with a safety net which will be designed to protect them from any type of security breach. The paper will also stress on the necessity of the application developers to remain proactive to identify future potential threats that may overpower the existing security system and prepare them accordingly. In case a data leakage is in place, there should be a proper mechanism to identify the leakage and amend it within a short period of time which will work as a damage control initiative. This paper will also discuss certain aspects that are closely related to gaining the trust of the users which may include a proper safety rating system that can be interpreted by the users. Secondly, there is a need to ensure that the apps are demanding for less permission which may assist with reducing the possibility of serious privacy violation in times of data breach.

DOI: 10.7176/IKM/10-2-07
Publication date: February 29th 2020

1 Introduction

We are living in the 21st century where the virtual world has become the heart of human civilization. Millions of people are now relying on the internet for using various types of high-tech devises that are being used for serving various purposes. With the emergence of smart phones, tabs and other sophisticated electronic devices, the use of different types of apps or programs has increased exponentially. These programs are being used for communication, data management, data sharing & processing, calculations and payment processing. A large portion of ecommerce is now being executed through the use of various types of apps. These apps are designed to make our lives considerably easier and secure.

2 Reasoned that affect the application security

With the number of users for these applications increasing exponentially, the risk factors are also increasing along. The main risk that has to be taken into account is the fact that the data can be accessed by a third party that does not have the legal authority to do so and often this access is done for securing financial gains, something that may lead to serious losses for the first party whose personal information is being accessed. Such actions can hamper the privacy of the user and at the same time can lead to severe insecurity which can hurt the usability of an application seriously. The very objective of making life easier for the general people can come under scrutiny.

These are the risk factors that are needed to be taken into account when it comes to administering the risk management governance of different applications. Over the years, the app developers have recognized the necessity of investing heavily for risk management. Different types of systems have been developed, tried and tested to serve the purpose. At the same time, there has to be relentless affords being made in order to have a clear understanding of the new threats that are coming to the market, something that had to be taken care of in order to ensure full security for the customers or clients.

There are both internal and external threats that are needed to be taken into account to serve the purpose. Research and development teams need to work relentlessly in order to develop systems or platforms that can be used in order to enhance the security of the applications so that perpetrators cannot penetrate and access the customer database. This entire process is highly complex and detailed which requires lots of research and study in order to establish a security system and at the same time, it also needs resources that can be utilized not only to develop an effective security system but at the same time to keep the whole team updated and relentlessly prepared for future threats.

Risk management governance for applications is a very complex process that enables the app developers to establish a governance system that would enable the IT experts to regularly monitor the present system to detect and prevent any form of security breach while at the same time, will also make sure that the right resources are being used in the right sectors in order to work relentlessly to develop better security systems that will enable the organization to develop new systems that can be used for enhancing the security of the apps in order to protect the organization itself and at the same time to ensure full security and maintenance of privacy for the users.

3. Literature Review

Sahd& Rudman, 2016 argued that one of the main reasons why risk management governance has become a vital issue in this day and age is because of the fact that the number of people who are using smart phones and other high-tech devices has increased significantly. There are millions of people all over the world who are using phones and it is found that near about 50% of the phones that are being sued by people in this day and age are smart phones (Gates, Chen, Li, & Proctor, 2014). And there are other high-tech devices that are needed to be taken into account including tabs and laptops. All these devices now use different types of applications that serve different purposes for the users. There are some apps that are being used solely for personal purposes. There are apps that are meant for entertainment whereas there are some others that are used for medical purposes. On the other hand, there are many apps available in the market that are being used for business purposes like maintaining a record of clients or customers, data processing, calculation, forecasting, record keeping and so on (Sahd & Rudman, 2016).

A large number of apps are being used for communication. These apps are being used for sharing different types of files that contain content based files as well as audio and video files. All these digital data contains confidential details that are being shared with other people. With the rise of users, there came different types of needs. And based on that, there have been different types of applications. Endless amount of data are now being stored through these apps and are being distributed among people. This naturally attracted a certain group of people who attempt to use those data illicitly for personal gains. So it has become mandatory for the developers of these apps to establish a highly detailed framework for security governance that will enable them to protect the best interest of millions of app users. A single breach can mean the possibility of a breach for thousands of users who are using the same app. Therefore, it is highly empirical to develop a security and system and maintain it carefully so that all the users can be protected in the best possible way.

When it comes to risk management governance for applications, one of the primary things that are needed to be taken under consideration is informing the users about the risk factors that are associated with the use of a particular application. There are rating systems and other mechanisms that are used by the application developers that are designed with the intention to inform the users about the possibility of their personal information being breached through any aggressive attempt made by the cyber criminals. However, often the risk factors are not clearly understood by the users since it requires adequate technical knowledge about the language and signs that come along with the applications that are meant to communicate the possible risk factors that are associated with the use of that application (Gates, Chen, Li, & Proctor, 2014).

Research has established that developing an easier channel of communication is mandatory for the app developers in order to grow awareness among the users which should be one of the mandatory factors in case of risk management governance. It is therefore important for the app developers to make sure that they are developing a system that will assist the users or potential users first to assess the risk level that is associated with a particular app. It is important to keep in mind that often many apps that come with similar functions seem to have similar safety concerns that follow a pattern. This is why, following an authentic system of properly rating the risk factors for the users are extremely important.

The integration of cloud computing, NFV and SDN, enables the IT experts to monitor and control the traffic when it comes to the use of the applications. This helps to have proper control over the data flow as well as the usability of different features of a particular app. In addition to this, the integration of SDN, cloud computing and NFV also make sure that the possibility of a data breach is being minimized through careful controlling of the traffic in order to monitor any unusual activity that does not fit the pattern. When it comes to risk management governance for different types of applications it is important to establish a monitoring system that will focus on any unusual activity which can be monitored precisely through the use of cloud computing with the combination of SDN and other technologies (Yan, Zhang, Vasilakos, 2015).

Cloud computing has been a technological aspect that has its implications for different vendors including Amazon, Google and Microsoft. All these IT giants have introduced the services associated with Cloud computing to provide a data processing facility that is trustworthy and comes with a stronger framework to offer identification and verifications processes. It is important to keep in mind that as far as the data management and prevention of data theft is concerned, the risk management governance needs to put a well-defined management system in place that does not only enable the users to enjoy a better platform for data management but at the same time reduces the risk of data leakage through the better utilization of a user verification system that is not quite easy to infiltrate by the perpetrators with the intention of illicitly using the data of the original users for their personal gain.

The separation of the hardware and software along with the concept of virtualized networks enables the risk management governance to be more secure through the utilization of a layer of securities that relies on the root trusted module (RTM), something that is very much proven to be effective to identify the authenticity of the access initiations generated by the users. The security layer carefully monitors the inputs produced by the user to identify whether he or she is the designated user who is meant to have access to the system for retrieving the data.

SFs are used by the modern security systems to identify the possible threats. They are also responsible for taking care of the malware infiltration and activate the protection system that cancels out any attempt executed by malware to infiltrate a specific target for accessing data that they are not meant to access without proper authentication. TFs on the other hand serve a different purpose. They are designed to identify the risk level for a particular source and also validated the trustworthiness of that source based on which, the recommendation is generated. So it is safe to say that this is more of a preventive measure that enables to identify the level of risk that a user may possibly get him exposed to while using an application for exchanging information of any kind (Yan, Zhang, Vasilakos, 2015).

One of the major themes of risk management governance implication is making sure that the possible risk factors are being identified beforehand during the time of the development of software. It is undeniable that when it comes to an online security breach, one of the primary sources of such violations is the weakness that comes along with the software itself. This can happen due to the weakness in different data storage facilities which makes it easier for the perpetrators to infiltrate the system. During the testing period, due to the lack of stable users, the software itself may not be tested properly which can leave weaknesses in the system (Shahzad, 2014).

On the other hand, the incompetence of the developers can also be a serious issue when it comes to developing the software. The developers are required to be well aware of the security issues and the methods that are being used by the hackers to breach the security layer of the software itself. They also need to be fully knowledgeable about the latest technologies that are readily available in the market that should be used for preventing such security breaches from happening.

Lack of management skills is also blamed sometimes for this which is often the case for software being marketed with security flaws that can be utilized by the hackers for their personal gains. The management's failure with planning and coordinating with the developers can lead to disastrous outcomes that cannot be prevented even if the team is skilled enough to develop software that will ensure maximum security for the users (Shahzad, 2014). Poor management of the resources as well as lack of communication among the team members and the management can lead to distance and misunderstanding, something that can be explained as the gap between the stakeholders which can enhance the risk of data breach.

So it can be said that one of the main function of risk management governance in applications should be establishing a sustainable infrastructure within the vicinity of the developers themselves which will allow them to develop software that is considerably more efficient in terms of safety measures. If the developers are competent enough and are highly knowledgeable about the latest security facilities and how they can be implemented in the software or application that they are making, it gives enough scope to amend the security weaknesses that can be abused by the perpetrators for hacking into the personal details of the users (Neves, et. al., 2014).

When it comes to risk management for software, one of the most important factors is knowledge management. This is important for having a clear understanding of the possible threats and how they are supposed to be mitigated by making the best use of the available technologies. This is a two way process where initially the developers gather enough knowledge about the possible threats that are already there which can expose the user of the software to the risk of data breach. How that breach was executed and what types of tools were used to serve the purpose is carefully analyzed followed by the detailed analysis of the point of breach. This enables the developers to understand the weaker points of the application which has to be taken care of for future breach attempts.

Gather knowledge about the potential new security measures as well as the threats is also important to come to a conclusion regarding the prevention techniques that should be adopted for risk management. Prevention reduces the potential losses that the user may suffer from while using an application. All the gathered knowledge is needed to be carefully examined and studied before the risk management affords can be designed with that knowledge in mind. Regression analysis, stochastic models and expert systems can be used for retrieving the data that is needed to come to a conclusion about the possible data breach situations or threats (Neves, et. al., 2014). Sensitivity analysis is also a very effective method that can be used to carefully assess the performance of an application when it comes to the careful analysis of its security layer that is meant to safeguard the users.

Risk management governance is often dependent oncareful analysis of a given scenario and how the elements of threats play their roles in the given circumstances in order to execute a security breach. This allows the observers to have a clear understanding of the capacity of the security layer to resist any data breach attempt. At the same time, it also allows them to understand the level of sensitivity that each element of security has against different elements that can be used for breaching the security (Neves, et. al., 2014). Based on the close observation of the scenario, the researchers can come to a conclusion about the possible steps that can be taken in order to overcome the weaknesses that an application may have.

Since the beginning of the 21st century, the world has witnessed the practice of outsourcing and global integration of software development to become one of the dominant models of application development. This mainly occurred as a part of the cost cutting measure which enables independent companies to outsource their production completely or partially to foreign developers who possessed the same skill levels like their domestic developers and would have charged lower for completing the tasks that they were meant to complete. This has been a major development in the IT sector in a time when the competition among the software development companies has increased drastically and one of the strategies for ensuring business stability was to introduce development projects that would be more cost effective some that the clients would have to pay less for the product that they wanted to have. The globalized access of information enabled different developing nations to acquire manpower for designing and developing applications that would help companies from the developed world to complete their projects for a reduced price (Verner, et. al., 2014).

However, the concept of global software development or GSD came with its limitations. First of all, the integration among the productions of experts from different countries turned out to be a highly challenging task due to the difference of methods and cultural philosophy. Often the concept of team work would not come into place to protect the collective interest of the company that developed the team which included experts from different countries. Sometimes the lack of understanding and gap between different parties led to weaknesses within the applications, something that would lead to hazardous consequences for the company as a whole with security breaches taking place. One of the first concerns for security for the development of a software or application is closely related to the idea of complete cohesion among the stakeholders. This would have made it possible to come up with a system that would be strong enough to overpower any security threats.

However, GSD did not allow that to happen in several circumstances where developing the applications for a lower cost received more importance than the idea of coming up with the most effective application that would strengthen the security system of the application so that the users' do not get compromised (Verner, et. al., 2014). One of the most important factors of successful risk management governance is the implication of a system in terms of application development that will ensure that all the parties are having a clear understanding of the standards and expectations from the management and what are the resources that are readily available for the teams to work with.

When different developers from different countries are scrambled to work on a single project, it is important to establish a strong line of communication in order to ensure better coordination among the team members. This enables to mitigate risk more effective as far as breach of security is taken into account. Historically it is proven that when the global teams manage to coordinate among themselves successfully, it can lead to the completion of application development processes more effectively that can yield better outcomes (Verner, et. al., 2014).

The use of mobile phones for healthcare has become more common in recent years than ever. The concept of Health or mobile health stresses on the idea of using different healthcare apps that enable the users to input their medical data which can be processed in order to deliver detailed analysis of the overall wellbeing of the user. Such applications can also be used for producing prescriptions for the users and to keep their records which can even be shared with professional health care service providers for retrieving data that can be used for diagnosis. The mobile health apps are designed to run on smart phones and other mobile electronic devices including tabs and pamphlets. In order to serve their purposes, these apps require the users to input various information about themselves which may include their blood pressure, daily diet and other activities (Chen, 2018).

4. Comparison between Apps (Some have high security and other does not

These apps can be divided into two broad categories in terms of their subscription- the paid ones and the non-paid ones. Most of the non-paid or free apps require more permission from the user in terms of accessing the devise. Based on the objectives of the app as well as the features that they cover, some apps may even access the camera, microphone and other features of a smart phone or electronic device that they are running into. This enables the apps to have access to highly sensitive and personal information of the user, something that can expose the user to the risk of an information breach (Sampat & Prabhakar, 2017).

5. The Importance of governance in Risk Management in Applications

If the security system of the app seems to have flaws, it can lead to the leakage of massive data that can be significantly sensitive by nature. There are laws available which make it mandatory for the caregivers to protect the details of the clients even in times of criminal investigations where the investigators may need court orders (Jing et. al., 2015). This is a clear indication of how sensitive such information can be by nature. This is when risk management governance comes into play which makes sure that these apps are utilizing state of the art IT security frameworks to make sure that no outside elements can breach into the personal profile of the users to access the sensitive information that can lead to serious problems for the user (Mesquida & Mas, 2015).

There are certain features that the apps should incorporate within their features which should make sure that the users have the power to determine exactly what type of information they are to share with the app and how they can control the ways the information can be managed and used by the developer and third parties. At the same time, the users should be provided with the authority to delete or change certain personal details that they have provided to the app database at the first place. These determine to what extent the developer is committed to respect and protect the privacy of the users and how they plan to protect their best interest (Lo, Yeh & Fan, 2016).

When it comes to the applications, one of the primary challenges for governance of risk management is to make sure that there is an effective system in place that is capable of detecting that there is a possible information leakage going on in the app. Often the safety measures turn out to be less effective to sense the possible data breach right at the first place to begin with which can make the problem worse (Huckvale, et. al., 2015). This is why governance of risk management needs to focus on two types of security measures, one for ensuring that the security layers are not being beached by any element and secondly to make sure that even if there is a leakage, that is being understood by the admin within a reasonable period of time so that the problem can be taken care of (Lo, Yeh & Fan, 2016).

Li, Tryfonas, Russell, Andriotis, 2016 suggested that “Multilayered Hierarchical Bayesian Network” is a major protection system that plays a vital role in the governance of risk management. There are several purposes this system is designed to serve. First of all, it focuses on the development of applications in a way that will make sure that any external forces are not being able to penetrate into the database of the users which can lead to a massive breach of security. At the same time, the network also initiates a complex security facility that is highly capable of identifying a data leakage and take actions in a timely manner in order to reduce the losses that may happen if the breach lasts for a prolonged period of time (Dini et. al.; 2018). To put it in s simple manner, the multilayered hierarchical Bayesian network focuses on ensuring full protection for the users through developing a multi-level barrier system that is designed not only to prevent a breach from taking place but at the same time to make sure that there are different systems in place that can take counter measures during the time of a possible breach or once the breach has already happened but is needed to be neutralized as a part of damage control (Zhu, Cao & Zhang, 2017).

6. Limitations

One of the primary limitations of this research paper is while it does cover the current threats and the available remedies that are available in the market for taking care of those risks, it does not provide a definitive answer to the question of whether the solutions are likely to ensure that a particular application is being fully secured from any kind of infiltration. However, considering the fact that the threats of new ways the data breach can be executed are a process that is being developed with consistency, it is not likely that a complete framework can be presented that can be described as the most effective way of preventing a possible data breach.

At the same time, the role the customers or users play in the security breach is not covered in detail in the paper. While it does offer the discussion about the options that are being provided by the developers in order to empower the users about the type of information that they can share with the developers and those they can avoid, it does not necessarily provide enough insight about how the lack of awareness and skills of the users leads to the breach of their personal information. It is highly empirical to keep in mind that when the data processing and storage is being used by a user, the level of education of that person plays an important role to determine the level of vulnerability of that person in terms of security threats. Based on that, the level of threat can be distinguished region wise where it is expected that countries with people who are more educated are likely to be more capable of following procedures that will safeguard them from different types of security threats. However, since the main focus of the paper has been the governance of risk management for applications, this may well be considered as a less prominent topic to be covered in detail.

7. Problem Statement

The main problem or challenge in this case is it is never easy to develop highly effective governance of risk management that can be used practically by the developers in order to establish a system that will reduce the data leakage to a maximum degree. At the same time, it is also a huge challenge to recognize how a sustainable team can be put together in order to develop a framework that can work effectively in order to make the best use of the available resources in more of a cost effective way that will justify the investment.

8. Security threats

There various types of security threats that can be taken into account when it comes to a breach for an application. First of all, it can lead to the perpetrators gaining access to highly sensitive information of the user that can be used for blackmailing the user or put him or her to a highly embarrassing situation which can be quite problematic. Secondly, this can lead to financial loss for the user if somehow the user’s debit or credit card or bank account details are being accessed by the perpetrator who then can lead to illicit financial activities like transferring fund from the victims account to an unknown location.

There is also the possibility of massive system collapse in cases if the data leakage leads to the perpetrator gaining access to the personal details of many users and then if the attacker deletes the information from the main database while downloading that in his or her own storage system. This can lead to massive disruption of services and can incur huge losses for the company that has developed the app.

Accessing the information of a user illegally or a database where confidential national security related information is stored can lead to unprecedented damages at a national and even international scale. This can expose the national security of a country significantly towards danger, something that should be avoided under any circumstances. It is vital to understand the possible threats that such breaches can lead to both from the personal, professional and national scale and grade them accordingly in order to identify the urgent issues that are needed to be addressed right at the first place to begin with.

9. Significant risks arising from apps

From the company perspective, one of the major strategic risks that a company may suffer from due to the data breach might be the exposure of the client list that can be used by the competitors provided that the perpetrator is working for the competitor or may approach the competitor in order to sell the information that he or she might have gathered through cyber-attacks. This may also hurt the brand image of the company or app developer itself which can lead to massive loss of customers or users. For instance, if the developer is renowned for ensuring the highest security for the users who are using the app, the breach of security can be a direct attack on the reputation of the developer, something that can lead to questioning his integrity. Another strategic risk can be the perceived sales can be disrupted significantly by the data breach due to the severe sense of insecurity that may arise in the mind of the customers, something that can lead to reduced number of people buying or downloading the app.

In terms of the operational risk, the data breach can disrupt the operation of the developer as it will be forced to invest its resources for risk management and damage control. Its resources will be put to a defensive approach in order to protect the integrity of the company instead of focusing on business development and expansion. On top of that, often such security breaches can lead to financial losses that can often occur through lawsuits being filed by the customers accusing the developer of failing to offer the best protection to them. The perpetrators can also inflict significant financial losses to the app developers through their infiltration of the security system.

10 A trust and security framework

When it comes to the usability of apps, there are two important elements that are needed to be taken under consideration. First of all gaining the trust of the potential users and secondly, making sure that the trust they put on the developer is being fully respected. With millions of smart phones and other electronic gadget users floating in the cyber world, there are thousands of apps that are hitting the market. However, not all of them are safe or designed to protect the best interest of the users. Based on historic data or previous experience about using an app, lots of users may feel skeptical about a particular application and may fail to understand its true potentials. It is therefore vital for the developers to build trust in the market so that people begin to use the applications developed by them without any hesitations.

One aspect of gaining trust is showing full respect to the privacy of the customers in order to make sure that they keep their confidence on the app. The rating systems should be utilized with utmost sincerity by the developers so that the users can have a clear understanding of the degree of reliability for the app. At the same time, the installation as well as the permissions should be requested keeping in mind the level of sensitivity of the information that is being asked from the potential users.

The customers should be assured that their information will be kept fully confidential and will not be sold to other third parties for financial gains by the developer. The privacy policy of the company has to be very clear and precise that should be developed based on the legal framework.

Once the trust is secured and the users are using the app with confidence, the risk management governance needs to play a vital role in order to make sure that the faith that the company has secured from the users is being respected and maintained by ensuring the best security for the users. The multi-layer security system is needed to be developed, implemented and monitored carefully. The possible risks are needed to be forecasted beforehand to take preventive measures. Like it has already been mentioned above, if a data breach actually does take place, it will be the responsibility of the management to neutralize the threat before it inflicts serious problems. There can be no alternative of that in order to protect the trust that the company has achieved from the users.

11 Methodology

In order to have a clear understanding of the concept of risk management governance for applications, scholarly articles and journals are going to be examined carefully to retrieve scholarly data. The peer reviewed sources will be used with accuracy to have a proper insight of the given problem and to understand where the works currently stand in terms of making a proper response to the given problem. Works of multiple authors are going to be taken and compared in order to validate the claims. While one of the basic elements of the foundation of this study is going to be secondary sources, the authenticity or credibility of the sources will make sure that they are giving a clear picture of the contemporary situation.

Many of the papers that are taken for references are those that have used primary data that has been collected in the most recent times. This is likely to give more reliability to the whole study.

12 Discussion

It is very much established that with the technological advancements, there has been a rise of users using smart phones and other high-tech electronic gadgets. With millions of people using these devises, there have been all kinds of applications emerging in the market that are designed to serve different purposes. Most of these apps demand the users share certain information with them. Some of this information is highly sensitive and can lead to disastrous consequences if they are falling in the wrong hands. There are many apps that serve the same purpose but some are better than others in terms of affectivity and security. At the same time, there are some apps that demand more permission than others which often exposes the user to the danger of data theft or in other words identity theft.

The risk management governance serves three important purposes for the app developers and users. This is a process that enables the development of a security system that is not quite easy to penetrate. At the same time, if there is penetration in play, the risk management system should be capable enough to get alerted about it which enables the security experts to take measures that will enable them to amend the breach within a short period of time. The governance of risk management for applications is required to play a rather proactive role in order to have a clear understanding of the possible threats that are likely to pose a threat to the industry.

13 Future works

The data management and security experts are working on developing a universal network that is likely to bring all the apps within a well-defined protocol which will enable the applications to become safer than ever. At the same time, there has been more focus on making the best use of the available resources in order to establish a framework that will be able to forecast a possible attack more accurately before it takes place. Access verification as well as real identity verification systems are becoming more biometric oriented which is likely to assist the users from being deceived or their personal information being violated by any sources from a distant location. Bigger companies like Facebook, Google, Apple and others are quite ahead than other app developers in this realm which has given them the scope of making the best use of research and technology to make their apps safer than ever for the users.

The result of this study is the conclusion that the number of application users is increasing at an unprecedented rate all over the world. This is why the governance of risk management has become even more important. In addition to that, the risk factors and the tools used by the perpetrators have also become more sophisticated which is why more resources are needed to be invested in the developing a safety net for the users.

14 Results

The results that can be taken into account based on the research is that with the number of smart phone and other gadget users rising, the risk of security infiltration has increased as well. Therefore, it has become even more challenging to ensure risk management governance that will not only safeguard the users but at the same time will work proactively for protecting them.

15 Conclusion

In conclusion, it can be said that a multi-layered security system with coordination with different IT experts needs to be taken into account to develop a highly integrated security framework. The elements of trust and safety should be connected and properly coordinated through the use of more sophisticated verification systems that will not only prevent the hackings from taking place but at the same time will forecast it more accurately for the app developers so that they can protect their users in the best possible way.

References

[1] Chen, J.; Wang, C.; He, K.; Zhao, Z.; Chen, M.; Du, R.; Ahn, G. (2018). Semantics-Aware Privacy Risk Assessment Using Self-Learning Weight Assignment for Mobile Apps.

[2] Dini, G.; Martinelli, F.; Matteucci, I.; Petrocchi, M.; Saracino, A.; Sgandurra, D. (2018). Risk analysis of Android applications: A user-centric solution.

[3] Gates, C.; Chen, J.; Li, N.; Proctor, R. (2014). Effective Risk Communication for Android Apps. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE 2014.

[4] Huckvale, K.; Prieto, J.; Tilney, M.; Benghozi, P.; Car, J. (2015). Unaddressed privacy risks in

accreditedhealth and wellness apps: a cross-sectionalsystematic assessment. Huckvale et al. BMC Medicine (2015) 13:214 DOI 10.1186/s12916-015-0444-y

[5] Jing, Y.; Ahn, G.; Zhao, Z.; Hu, H. (2015). Towards Automated Risk Assessment and Mitigation of Mobile Applications. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 5, SEPTEMBER/OCTOBER 2015.

[6] Li, S.; Tryfonas, T.; Russell, G.; Andriotis, P. (2016). Risk Assessment for Mobile Systems Through a Multilayered Hierarchical Bayesian Network. IEEE TRANSACTIONS ON CYBERNETICS, VOL. 46, NO. 8, AUGUST 2016.

[7] Lo, N.; Yeh, K.; Fan, C. (2016). Leakage Detection and Risk Assessment on Privacy for Android Applications: LRPdroid. IEEE SYSTEMS JOURNAL, VOL. 10, NO. 4, DECEMBER 2016.

[8] Mesquida, A.; Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension.

[9] Neves, S.; Silva, C.; Salmon, V.; Silva, A.; Sotomonte, B. (2014). Risk management in software projects through Knowledge Management techniques: Cases in Brazilian Incubated Technology-Based Firms. International Journal of Project Management 32 (2014) 125–138.

[10] Sahd, L.; Rudman, R. (2016). Mobile Technology Risk Management. The Journal of Applied Business Research – July/August 2016 Volume 32, Number 4.

[11] Sampat, B.; Prabhakar, B. (2017). Privacy Risks and Security Threats in mHealth Apps.

[12] Shahzad, B. (2014). Identification of Risk Factors in Large Scale Software Projects: A Quantitative Study. International Journal of Knowledge Society Research, 5(1), 1-11, January-March 2014.

[13] Verner, J.; Brereton, O.; Kitchenham, B.; Turner, M.; Niazi, M. (2014). Risks and risk mitigation in global software development: A tertiary study. Information and Software Technology 56 (2014) 54–78.

[14] Yan, Z.; Zhang, P.; Vasilakos, A. (2015). A security and trust framework for virtualized networks and software-defined networking.

[15] Zhu, X.; Cao, C.; Zhang, J. (2017). Vulnerability severity prediction and risk metric modeling for software