Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-14-2013

Managing Risks in Crowd-Funding Platforms

Alvaro E. Arenas
IE University, alvaro.arenas@ie.edu

Manan Podar
IE University, mkpodar.phd2016@student.ie.edu

Prasad Dalvi
IE University, pdalvi.imba2014@student.ie.edu

Managing Risks in Crowd-Funding Platforms

Alvaro E. Arenas[1]
Information Systems and Technologies
Department, IE Business School, IE University,
Madrid, Spain

Manan Podar
Information Systems and Technologies
Department, IE Business School, IE University,
Madrid, Spain

Prasad Dalvi

Information Systems and Technologies
Department, IE Business School, IE University,
Madrid, Spain

ABSTRACT

The purpose of this paper is to analyze risks in crowdfunding platforms. In crowdfunding, a network of people pool their money, usually via the Internet, in order to invest in and to support efforts initiated by other people or organizations. We follow a case study approach by applying the CORAS risk management methodology to the Appbackrcrowdfunding platform. This research addresses two research questions: How suitable is the CORAS methodology to analyze risks in crowdsourcing platforms? What are the main risks in a crowdfunding platform? The findings reveal potential threats and risks for the main stakeholders in crowdfunding platforms, and a set of risk treatment strategies are derived for the key risks.

Keywords: crowdfunding, open innovation, risk management, CORAS methodology

[1]Corresponding author: alvaro.arenas@ie.edu.

INTRODUCTION

Crowdfunding is a method of financing in which, a network of people club their money together towards the goal of investing in or supplementing efforts initiated by other people or organizations (Ordanini, 2009). These network efforts usually happen over the Internet.

Crowdfunding initiatives have gained popularity in various markets; notably, SellaBand and Catwalkgenius in the music and fashion sector respectively, Kickstarter in the manufacturing sector, and Appbackr in the application development sector, among others.

Crowdfunding can be seen as an evolution of the crowdsourcing concept where the crowd contribution to the firm's production process is done by providing the financial resources required for the execution of the project instead of or in addition to providing ideas for improvement of the project (Kleeman et al., 2008). The purpose of this paper is to analyze risks in crowdfunding platforms. Our aim is to determine the main type of risks present in crowdfunding platforms. We have followed a case study methodology; selecting one of the previously mentioned platforms - Appbackr - and analyzing its potential risks using the CORAS risk management methodology (Lund et al., 2011).

The selection of Appbackr has been motivated by it being the first crowdfunding platform developed for mobile applications; it has had a steady growth in recent years, including interesting features such as a marketplace where developers can sell developed apps to wholesale buyers, and managing the reputation of all their applications via reviews from users. On the other hand, the selection of CORAS was motivated for being a framework based on recognized standards such as the ISO 31000:2009 standard for risk management, integrated with constructors to analyze non-technical risks such as legal risks.

The structure of the paper is the following. Next section reviews the literature on crowdfunding and risk management, followed by an overview of the CORAS methodology. Then, CORAS is applied to the Appbackr platform. Finally, we discuss our findings, draw some conclusions, and highlight future work.

LITERATURE REVIEW

Due to the possible business or strategy change inherent to the phenomenon, innovation always brings risk (Souza et al., 2009). According to Araki and Lang (Araki & Lang, 2007) the key risk factors that should be considered in open innovation are investment risk, development risk, co-ordination risk, motivation risk, control risk, security risk, governance risk and culture risk. Extending this theory, researchers have suggested that intellectual property risk should be added to this list for crowdsourcing platforms (Souza et al., 2009). Since crowdfunding platforms are an extension of crowdsourcing open innovation platforms, we believe that all these risks could be inherent to crowdfunding platforms.

However, crowdfunding may put more risk on the consumer than other open innovation platforms. Rather than buying the product, they pay for producing or promoting a product and bear the risks associated with it. This evolved role of the consumer brings to fore its entrepreneurial and social networking skills (Ordanini et al., 2011). Selecting projects to invest in and deciding on the size of the investment count towards the entrepreneurial side of crowdfunding. Making sure that the selected project gains popularity among other investors counts towards the social networking side of crowdfunding. Therefore, in addition to the above

mentioned risks, we postulate that due to the nature of the platform there could additionally be two very important risk factors: financial risk and legal risk.

Tackling these risks requires a company to manage them in advance by understanding their impact and nature, anticipating their occurrence by monitoring indicators and being ready to take action at the first signs of trouble. These actions constitute risk management practices.

AN OVERVIEW OF THE CORAS FRAMEWORK

A risk management approach should be applied in any situation where there exists a possibility of loss, or of opportunities, at the strategic or operational level. Several risk management methods for the context of IT systems have been proposed in the past. We chose to concentrate on the CORAS approach, which was developed initially for the analysis of security-critical IT systems (Aagedal et al., 2002), and then extended to include contractual and legal risks (Mahler &Vraalsen, 2006).

The CORAS approach consists of a method, a graphical language, and a computerized support tool for risk analysis. The biggest benefit of the CORAS method, set on the ISO 31000:2009 standard for risk management, is that it blends state-of-the-art system modeling methods based on UML 2.0 seamlessly with various aspects from different risk analysis techniques giving us a powerful tool (Lund et al., 2011). They main motivation behind using a model-based risk assessment approach like CORAS is to improve the descriptions of target system, as well as to obtain a better communication and interaction between stakeholders involved, better documentation of results and assumptions enabling possible reuse. All of these

benefits resonate with our case under consideration helping us determine that using the CORAS approach perfectly fits our needs.

The method follows a structured and systematic process directed by assets, as illustrated in Figure 1. The graphical language covers basic notions of risk analysis, as depicted in Figure 2.

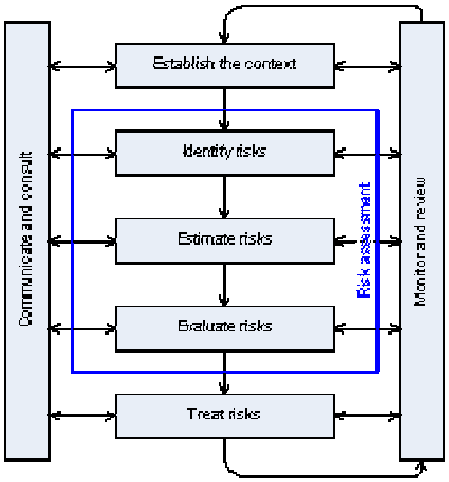

Figure 1. Risk analysis method.

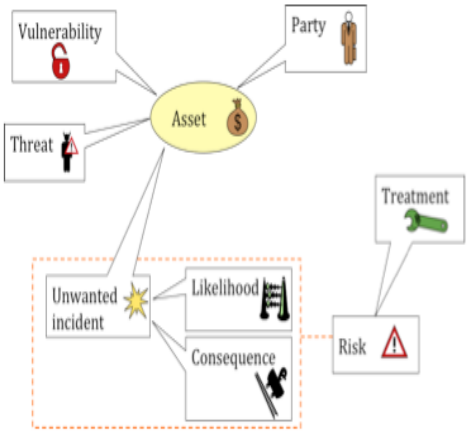

Figure 2. CORAS graphical language.

In the context of CORAS (Lund et al., 2011), an asset is something to which a party assigns value and hence for which the party requires protection. A threat is a potential cause of an unwanted incident. A vulnerability is a weakness or deficiency that opens for, or maybe exploited by, a threat to cause harm to or reduce the value of an asset. Risk is defined as the likelihood of an unwanted incident and its consequence for a specific asset. A treatment is an appropriate measure to reduce the level of value of a risk.

Due to limitation of space, in this paper we will concentrate on the risk assessment part, in particular risk identification, and will propose some risk treatment strategies.

APPLYING CORAS TO APPBACKR

An Introduction to Appbackr

Appbackr acts as an online wholesale market providing funding and distribution for new apps to various mobile operating system platforms and application stores. There are 5 participants in the Appbackr business model: (i) The Developer develops the application (prototype) and requires funding to finish the development and/or for marketing (ii) The Backr invests in apps that are of interest to him by pre-buying copies of the application at a discount (iii) The Customer buys the final application from the application stores (Apple Appstore, Google Play, etc) (iv) The Appbackr platform provides the medium for the transactions to happen (v) The Application stores are the platforms where the applications are sold to the Customer.

Appbackr provides a marketplace that connects Developers and Backrs. The Developer who needs funding decides to publish his application on the marketplace. Backrs can search the marketplace and buy copies of one or many apps published by various developers at a discount. Appbackr decides this discounted price. The revenue from these Backr purchases is given to the Developer with a small commission charged by Appbackr. The Developer can use the money received from the sales however it wishes: for development, marketing, etc. There is no commitment of future sales on the part of the Appbackr towards the Backrs.

When the platform-approved apps of the Developers are ready to be sold on the application stores, the Developer has two choices. He can either publish the application on the application stores directly, or he can use the Appbackr platform to help him publish on the

application stores. Appbackr earns money on a commission basis for providing and maintaining its platform and ensuring all the transactions are run smoothly without any conflict.

Risk Management in CORAS for Appbackr

To apply the CORAS methodology to Appbackr, the first step was to understand the business model for Appbackr as a firm. This was done by analyzing and understanding the publically available information on the Appbackr website. Understanding the business model first and then performing the risk analysis helped us answer some important questions about the various events and transactions that occur as part of the Appbackr process flow and to establish the context for risk analysis.

As part of actual application of CORAS to Appbackr we considered risks for three stakeholders: the Developer, the Backr and the Appbackr platform, as these are the primary stakeholders of any crowdfunding project.

For the Developer, threat analysis is illustrated in Figure 3, and the potential treatment alternatives can be described as follows. The non-human threat that a developer faces with Appbackr is that his/her application may not sell enough in the Marketplace. This can lead to one of two unwanted incidents: (i) the application cannot be completed due to lack of funding; or (ii) the application development is delayed due to lack of funding. The vulnerability in both cases is that there is no other source of funding available for the Developer since he may be relying solely on the Appbackr funding in the form of sale of copies to Backr community.

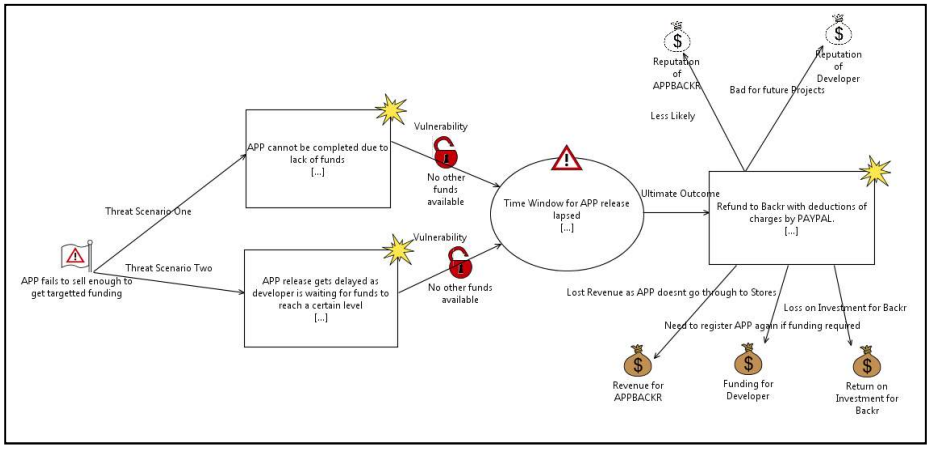

Figure 3.Threat Analysis for AppBackr Developer.

These incidents along with the associated vulnerability will thus lead to a threat scenario where the time window of 45 days (30 day release period and a 15 day allowance) (AppBackr 2010) for application release will lapse. This leads to another unwanted incident where the Backr, who has bought the application already, will be refunded the money by Paypal, but only after deducting certain handling charges. This will cause losses to multiple assets: indirect asset losses via loss of reputation for Appbackr and the Developer, and direct asset losses via loss on investment for Backr, loss of funding for the Developer, and loss of revenue for Appbackr.

A treatment to these risks lies in the change by Appbackr in its business model. Since October 2012, the platform changed its business model from supporting concept apps which meet their target reserve goal, to supporting pre-release apps which are ready for the app stores (AppBackr 2010). With this shift in business model, Appbackr has created an implicit assurance from the Developers to the Backrs that their investment is secure, reducing the vulnerability associated. It also changes focus from funding to develop an app to funding for distribution and marketing of an app, as the developer would use most of the money earned for deciding the

distribution strategy for the already-developed app. Addressing the vulnerability is one of the ways to treat the risks identified by CORAS threat analysis.

The threat analysis for the Backr is illustrated in Figure 4, and the potential treatment alternatives can be described as follows.

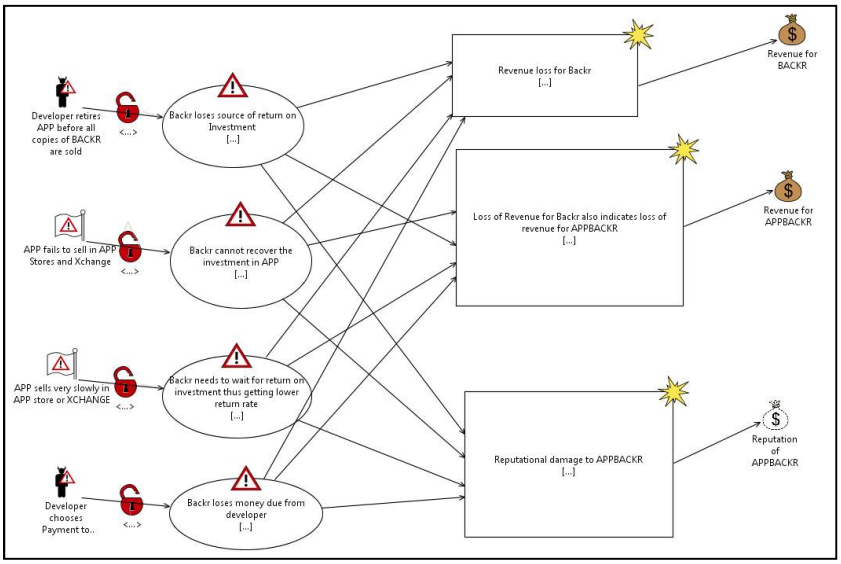

Figure 4.Threat Analysis for Backr in AppBackr.

The non-human threats that a Backr faces with Appbackr are: (i) the application for which he has bought copies may sell slowly on the application stores; and (ii) the application may not sell at all. Additionally, Backr also faces human deliberate threats posed by Developers: (iii) if the Developer decides to retire the application from application stores even before all copies of the Backr have been sold; and (iv) if Developer chooses to get revenues directly from the application stores and redirect the share of Backr and Appbackr from his account, but does not actually do so.

These non-human threats can lead to threat scenarios where slow sales will reduce the rate of return on investment for the Backr and no sales will lead to loss of the profit and the

investment. The human deliberate threats can lead to threat scenarios where retiring the application can cause permanent loss of revenue for the Backr and the non-payment by Developer can cause reduced earnings and may involve legal proceedings, which can be costly.

Thus, the risk profile for Backr is different from that of the Developer as there are more threats involved, and additionally, there are human threats that create a direct vulnerability leading to various threat scenarios. These threat scenarios lead to one of the three unwanted incidents: revenue losses for Appbackr, lost investment for the Backr, and reputational damage for the Appbackr. Each of these incidents in turn leads to a loss of corresponding assets.

In terms of a treatment scenario, the smart app algorithm by Appbackr is an useful tool to analyze and rate all pre-release apps. Once any app gets the required mandatory rating of 8.5+ out of 10, it signals the market and the various app stores about the higher quality and credibility of the app. Tie-ups of Appbackr with various leading app stores and its own Xchange store ensure that there is sufficient exposure for good apps. These current aspects of the business model of Appbackr serve as a treatment for risks mentioned above (AppBackr 2010). Apart from these, we also suggest that Appbackr may increase use of its social media portals e.g. the facebook page (AppBackr 2010) to promote its apps. Currently, Appbackr is using this medium only to communicate with developers, but the viral effect that social network campaigns can have would serve as a good promotion strategy.

For the Appbackr platform, the threat diagram is illustrated in Figure 5, and can be considered as an accumulation of threats for Developers and Backrs. These follow the same flow as described with respect to the Developers and Backrs and can have similar potential treatments.

Once the various risks are identified and the related threat scenarios are integrated with different assets, estimated probabilities (likely, not likely, etc.) can be allocated to each threat

scenario. These various scenarios, their corresponding probabilities and associated assets impacted, help us to understand the extent of risk. CORAS allows linking of various treatment scenarios associated with each threat, thus helping to evaluate whether the risk is manageable and if yes, at what cost.

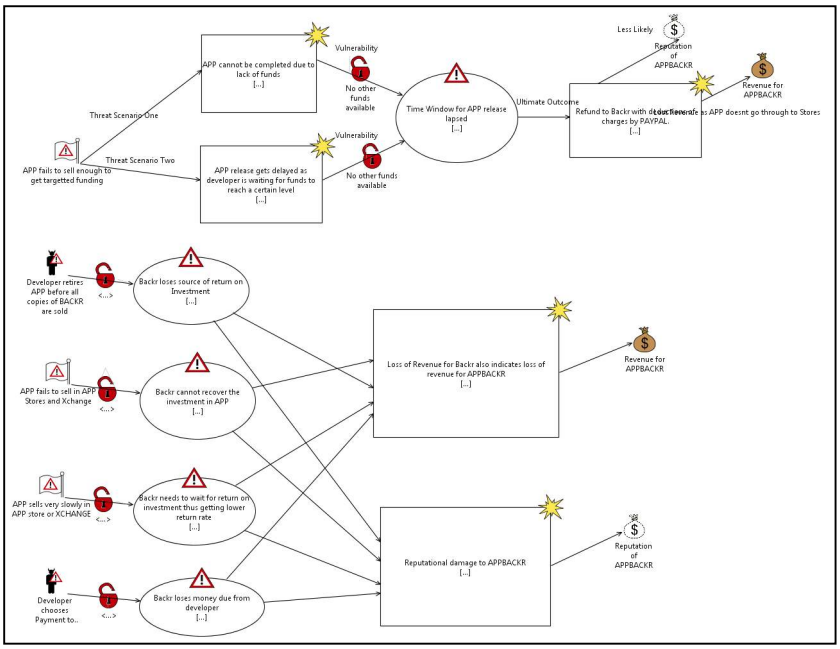

Figure 5.Threat analysis for AppBackr platform.

DISCUSSION

From our literature review, we noted that most studies on risks in open innovation / crowdsourcing focuses on identifying a list of risk factors (Souza et al., 2009); (Chou & Chou, 2011). In most cases, it is not determined where the risks are coming from, or they are presented in a general way. The systematic process followed by CORAS helped us in getting into more detail about the potential risks, revealing threat scenarios and their impact on assets.

The three types of stakeholders analyzed in AppBackr are typical of crowdfunding platforms: the subjects, Developers in AppBackr, propose new projects that require funding; the supporters, Backrs in AppBackr, form a group of people or organizations that decides to

financially support these projects. Supporters bear the risks of the investment in return for some expected payoffs, tangible and/or intangible. Crowdfunding platforms bring together subjects and supporters, and facilitate smooth communication between them (Ordanini et al., 2011).

The main threats and risks identified for crowdfunding could be summarized according to the type of stakeholders. For the supporters one threat is that subjects suspend their project/product or the commercialization of the project/product is not as successful as expected, reducing the expected return on investment for the supporter and affecting the platform reputation. For the subjects the main risk is the lack of funding, which will again affect supporters and the platform. The platform managers need to contribute in mitigating supporter and subjects risks by designing strategies to tackle such risks, as was exemplified for the case of AppBackr.

One difference between the identified risks for crowdfunding and the risks usually mentioned in crowdsourcing is the management of intellectual property (IP) (Souza et al., 2009). In our study, IP management did not appear as a meaningful threat, since usually the IP belongs to the developer and the supporter is getting predetermined revenue according to his investment.

In relation to the CORAS methodology, we found that CORAS can be particularly useful in the case of crowdfunding platforms due to its ability to trace and relate all probable threats for each stakeholder. Although not exploited in the paper, the combination of technical and legal risks as part of the methodology makes it suitable for analysis crowdfunding platforms.

CONCLUSIONS AND FUTURE WORK

This paper applies a risk management methodology to a crowdfunding platform for the purpose of identifying main risks for several stakeholders in the crowdfunding model: the subjects, authors of new projects to be funded; the supporters, investors in the projects; and the platform provider, connector for subjects and supporters. The analysis was carried out on AppBackr, a popular crowdfunding platform for funding the development of mobile applications, using the CORAS risk management methodology.

The analysis has focused on the risk assessment part of CORAS, especially in risk identification. We have identified several types of risks for the main stakeholders in crowdfunding and proposed mitigation strategies for some risks.

The work reported here is part of a more ambitious project developing risk management strategies tailored for open innovation platforms. An important part in the project is a catalog of main risks in open innovation platforms and its corresponding mitigation strategies, and this work is a part of such endeavor. We are currently applying CORAS to other crowdfunding platforms in order to contrast their risks with the ones identified for AppBackr.

REFERENCES

Aagedal, J. O., F. den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, K. Stolen. "Model-based Risk Assessment to Improve Enterprise Security". Enterprise Distributed Object Computing Conference. Lausanne, (2002). 51 - 62.

AppBackr. Facebook Page. 05 March 2010. https://www.facebook.com/appbackr.

AppBackr. FAQ. 2010. http://www.appbackr.com/faq.

Arakji, R. Y., K. R. Lang. "The virtual cathedral and the virtual bazaar". The Database for Advance in Information Systems 38, Nov 2007: 33 - 39.

Chou, D. C., A. Y. Chou. "Innovation outsourcing: Risks and quality issues". Computer Standards & Interfaces 33, 3, (2011): 350 - 356.

Kleeman, F., G. G. Voss, K. Rieder.Un(der)paid innovators: the commercial utilization of consumer work through crowdsourcing. Science, Technology & Innovation Studies 4, 1(2008): 5 - 25.

Lund, M. S., B. Solhaug, K. Stolen. Model driven risk analysis: the CORAS approach. Springer, 2011.

Mahler, T., F. Vraalsen."Legal Risk Management for an E-Learning Web Services Collaboration". Sylvia Mercado Kierkegaard. Oslo, (2006): 503 - 23.

Ordanini, A. "Crowd funding: customers as investors." The Wall Street Journal, 23/03, 2009.

Ordanini, A., L. Miceli, M. Pizzeti, A. Parasuraman. "Crowd-funding: transforming customers into investors through innovative service platforms". Journal of Service Management 22,4 (2011): 443 - 470.

Souza, L., I Ramos, J. Esteves. "Crowdsourcing Innovation: A Risk Management Approach". 2009.