The Impact of IT Risks on the Development of Innovative Start-Up of Mining Enterprises

Ryszard Pukala[1], and *Ivars* Linde[2]

[1]Bronislaw Markiewicz State Higher School of Technology and Economics in Jaroslaw, Czarnieckiego St., 16, 37-500 Jaroslaw, Poland
[2] ISMA University, 1 Lomonosova Str., Bld.6, LV-1019, Riga, Latvia

Abstract. This study aims at presenting IT risks, the materialization of which can have impact on business activity of innovative enterprises, including start-ups. We need to emphasize that such enterprises are largely associated with the use and implementation of modern technologies in various sectors of the economy. We also need to underline that enterprises of this type to an ever-greater extent act as an impulse triggering innovativeness of the economy as seen from the national and international perspective. Therefore, risk limitation in the enterprise development process, especially in the field of IT, may be an element that supports reaching the product scaling stage and working out an optimal business model, which stands as a chance of achieving market success and competitive advantage. As indicated by researchers, start-ups identify IT risks within the area of their activity and undertake actions aimed at limiting them.

1 Start-ups as innovative enterprises

The notion of innovation is a subject of focus of various scientific disciplines; therefore, it is hard to come up with a single universal definition. This issue was put under analysis already in the middle of the previous century. It was then J.A. Schumpeter defined innovation as [1]:
• introduction of a new product,
• introduction of a new production method (process innovation),
• opening of a new sales market,
• opening of a new supply market,
• introduction of a new organisation.

The abovementioned five types of innovation indicate that it was (and continues to be) identified as novelty introduced in the domain of business operation of an enterprise.

In the following years innovation was subject to research carried out by an ever-broader circle of scientists, which allowed formulating a comprehensive definition of an enterprise whose operation may be classified as innovative. J.A. Allen [2] claimed that innovation was the introduction of new products, processes or ways of conduct into wide use, while P.R. Whitfield indicated that innovation was every modification based on the assimilation of

[1] Corresponding author: m.petrova@ts.uni-vt.bg

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

transferred knowledge [3]. E.M. Rogers' definition of innovation as the introduction of new products, processes or ways of conduct into wide use is also very broad in meaning [4]. H.G. Barnett, however, defined innovation differently, relying on an assumption that it encompassed every concept, idea, attitude, stance or object that stood out among all previously existing ones owing to its quality. Innovation is also explained as a process of creative use of knowledge, transformation of knowledge possessed by an organisation or acquired from outside to be used in new products, services or processes [6]. The presented standpoints are only a few among a myriad of definitions formulated by a large group of scientists who have dealt with this issue. In this field we can distinguish pieces of work Pukala [7, 9], Pukala&Petrova [8], Kurmanov et al [10], Seitzhanov et al [11], Mussapirov et al [12], Petrova et al [13], whose multi-layered analyses of innovation have enriched and expanded knowledge in this scope.

Based on these definitions we can explicitly declare that start-ups can be classified as innovative enterprises. Without getting into details of numerous definitions of such enterprises, it is worth however to mention one of the most popular classifications: according to Blank, a start-up is a temporary organisation that strives at achieving a profitable, scalable and repetitive business model [14, 15]. While making the concepts of such enterprises more general, it is worth concentrating on their characteristic features, which include [16]:

• a lack of history – young companies can exhibit only a short operating history and many of them have very limited historical financial data at their disposal,
• modest income or a lack thereof or losses from operation – limited financial data become even less useful due to a poor information content and a permanent loss from operation.
• dependence on foreign capital – in the early phase of operation start-ups are usually financed from owners' own funds, EU funds or private investor funds (Venture Capital, Business Angels and other funds),
• considerable risk of failure – most young companies are incapable of succeeding in launching a product on the market.

Regardless of the approach, the activity of business entities operating on the market is currently a key instrument for boosting economic growth and innovation of the economy. Innovative enterprises are a significant part of this process. We can classify variously defined start-ups to this very group, as they – through their innovative undertakings aimed at delimiting their unique developmental path – can quickly take national and global markets by the storm, since they cover all aspects of modern life.

2 IT risk faced by start-ups

A risk is an indispensable component of each business activity and can be defined in various ways, both in theoretical and practical terms. However, risk is mainly associated with entrepreneurship and is reflected in the classical and neoclassical theory of entrepreneurial risk.

Information technologies belong to the crucial aspects dealt with by most enterprises, whose correct functioning depends on the efficiency of IT systems. This is a particularly important element of the operation of start-ups, as the vast majority of them use modern IT technologies and solutions to conduct their business activity and reach out for their clients.
The concept of IT (cybernetic) risk is usually understood as uncertainty with regard to the use of information technologies within an enterprise. IT risk, both in business and financial industry, increases proportionately to an increasing interdependence between an organisation, clients, partners and outsourced operations. As regards start-ups, this type of risk is of particular importance, as these enterprises make use to a great degree of advanced information technologies and tools on an everyday basis. Therefore, this type of risk has a

fundamental impact on the operating activity of an enterprise. In this context, it is worth mentioning a definition of cybernetic risk coined by a group of researchers led by A. Mukhopadhvay, according to whom it is a risk of emergence of adverse electronic events that can disturb business operation or trigger financial losses [17]. Therefore, this approach directly links this type of risk to the operating activity of start-ups. However, this notion is far broader and deeply embedded in the field of security of information owned and processed by an enterprise [18]. Processes employed by start-ups use a broad spectrum of devices and procedures, whose main aim is to develop and build value. Seen from this perspective, it is worth referring to a definition presented by R. Böhme and G. Kataria, according to whom it is a risk of disturbance of information systems [19]. A popular definition of the cybernetic risk has been formulated by J.J. Cebula and L.R. Young, who claim that this is an operating risk appearing in the sphere of information and technological resources of an organisation, the adverse effects of which can have impact on confidentiality, availability and integrity of information or IT systems [20]. They have distinguished between four classes of IT risk sources, namely [20]:
• human activities,
• disturbance in IT systems and devices operation,
• inefficiency of internal processes at an organisation,
• external incidents.
The cybernetic risk is most often classified by a type of detrimental activities that lead to the materialisation of losses, i.e. causes of cyber-damage. According to the systematics developed by the Governmental Computer Incidents Response Team (Poland), the causes of cyber-risk can be divided into intentional and unintentional (accidental). Intentional actions include [21]:
• injection of malware (virus, bug, trojan, dialler, botnet),
• security circumvention (unauthorised logging, account compromise/web attacks, application compromise),
• contents published on the Internet (offensive content, libellous/slanderous content, violation of copyrights, misinformation),
• illegal collection of information (scanning, interception, social engineering, spying, spam),
• computer sabotage (unauthorised alteration of information, unauthorised access, unauthorised use of information, DDoS access denial, data scanning, taking advantage of device and application vulnerability),
• human factor (violation of security procedures, violation of applicable laws),
• cyberterrorism (terrorist acts committed in the cyberspace).
• Unintentional actions in the cyberspace have been divided into two categories:
• random accidents and incidents (device failures, connection failures, software errors),
• human factor (violation of procedures, negligence, incorrect device configuration, lack of knowledge, violation of copyrights).
However, regardless of the classification, all IT risks have a very significant impact on start-up operation, since modern IT solutions and the use of new technologies form the basis of their development [22].

3 Impact of IT risks on start-ups

While studying Polish start-ups, 8 most important IT risk categories have been singled out[1]. The following ones have been defined by start-up owners as having key importance:
• IT systems failure

[1] *The study was conducted among 200 start-ups in October and November 2018.*

• loss of intellectual property/sensitive data,
• computer crime/hackers/viruses,
• a lack of adequate IT infrastructure,
• inefficient antivirus/antispam systems,
• problems related to computer devices in stock,
• problems related to software and licences,
• dependence on IT service suppliers.

The results of conducted analyses indicate that the broadly understood risk of IT system failure poses the greatest threat to start-ups, but it also depends on a stage of development and time of a start-up's presence on the market – Fig. 1.

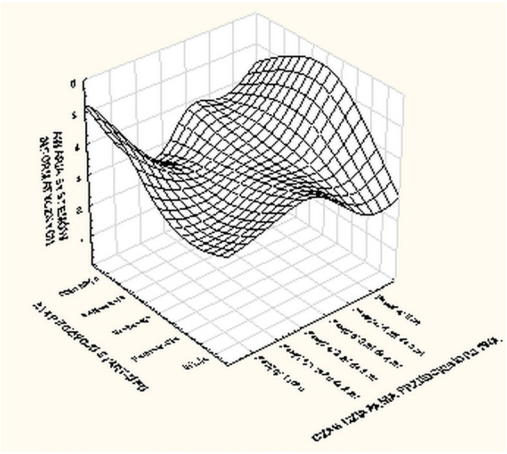

Fig. 1. IT risk assessment – differences depending on the time of operation and developmental stage of a start-up.

The chart topography indicates that the IT system failure represents the greatest threat for start-up operation. It has the following impact as defined by start-up representatives:

1. Maximum (5 pts) – for start-ups operating for up to 1 year and in the scaling and maturity phase and for start-ups operating for over 4 years and in the validation and scaling phase. The presented indications certainly derive from a situation in the developmental process of start-ups that usually treat the first year of operation as a breakthrough in striving towards market success, therefore any problems related to operation may undermine their future. When it comes to the other group (operating for over 4 years), this is a de facto "to be or not to be" struggle, for if a given entity has not managed to reach maturity within such a long period, then the chances for success fall dramatically and materialisation of IT risk can only exacerbate problems.
2. High (4 pts) – for start-ups operating for between 1 and 2 years and in the scaling and maturity phase as well as for start-ups operating for over 4 years in the validation, scaling and maturity phase. In this case, similarly as above, for start-ups operating for between 1 and 2 years and in the scaling and maturity phase, this is usually a breakthrough moment of entering the business stability stage. Any turbulences in this sphere may delay the process. For start-ups operating for more than 4 years and in the validation and scaling phase, this is a struggle for survival, while for the ones in the maturity phase, it is an element of achieving business stability and market success.
3. Low (2 pts) – for start-ups operating for up to 3 years and in the vision, forming and validation phase, for start-ups operating for between 2 and 3 years and in the scaling and maturity phase and for start-ups operating for over 4 years and in the vision phase. Start-ups in the abovementioned phases and developmental stages either continue the process of

reaching the product scaling stage, therefore they are less dependent on IT, or – as with the ones already in the maturity phase – they asses their security measures and operating readiness as the one that allows conducting business activity without interruptions, even if IT risks materialise.

We need to note that IT risk in start-ups grows along with the degree of interdependence between an organisation, clients, partners and outsourced operations. Frequently though, when commissioning the performance of a given service, a start-up provides a contractor with an access to an internal IT system to a degree that is necessary to perform work, but at the same time lacking important tools that could verify the contractor's actions.

Unfortunately, such a solution may be used by contractors to cover errors, install malware, cause other types of damage or to intentionally output data concerning clients or solutions that contribute to achieving competitive advantage of a given enterprise over others. Therefore, start-ups should by all means undertake actions aimed at limiting the impact of IT risks on their business activity, since abandoning them may cause irreversible problems with their development and thwart market success.

4 Summary

Due to conducting their business activity in various fields of new technologies and striving to reach maturity and competitive advantage, start-ups face a possible materialisation of risks that can destabilise or even prevent their development. Out of a vast collection of risks, the emergence of IT risks can pose a serious threat for the development of start-ups, since they rely to a great extent on modern technologies. Therefore, this awareness requires them to monitor IT risks on an ongoing basis and, if possible, to use tools that allow limiting them (e.g. insurance). Only sustainable development of start-ups, on the one hand taking into account high operating risk and insolvency as its possible consequence, and on the other hand considering development chances and possibilities created by the market, will make these enterprises become successful in business terms.

References

1. J. A. Schumpeter, *Theory of Economic Development* (PWN, Warszawa, 1960)
2. J. A. Allen, *Scientific innovation and industrial prosperity* (Longman, London 1966)
3. P. R. Whitfield, *Innowacje w przemyśle* (PWE, Warszawa, 1979)
4. E. M. Rogers, *Diffusion of innovations* (Free Press, New York, 2003)
5. P. F. Borowski, Europejski Doradca Samorządowy, **17:2**, 24, (2011)
6. D. Cavagnoli, Innovation: Management, Policy and Practice, **13**, 4 (2011)
7. R. Pukala, Economics and Management, **8:3,** 1 (2016)
8. R. Pukala, M. Petrova, E3S Web Conf., **105**, 04034 (2019)
9. R. Pukala, E3S Web Conf., 105, 04015 (2019)
10. N. Kurmanov, M. Petrova, S. Suleimenova, E3S Web Conf., **105**, 04045 (2019)
11. S. Seitzhanov, N. Kurmanov, M. Petrova, U. Aliyev, N. Aidargaliyeva, Entrepreneurship and Sustainability Issues, **7:4**, 2615-2629 (2020)
12. K. Mussapirov, J. Djalkibaev, G. Kurenkeyeva, A. Kadirbergenova, M. Petrova, L. Zhakypbek, Entrepreneurship and Sustainability Issues, **7:2**, 1480-1495 (2019)
13. M. Petrova, O. Sushchenko, I. Trunina, N. Dekhtyar, *Big Data Tools in Processing Information from Open Sources* (SAIC, Kyiv, 2018)

14. S. Blanc, B. Dorf, *Podręcznik start-upu. Budowa wielkiej firmy krok po kroku* (Helion, Gliwice, 2013)
15. O. Baklanova, M. Petrova, V. Koval, Economic Studies, **29:1**, 68-91 (2020)
16. A. Damodaran, *Start-up and Growth Companies: Estimation Issues and Valuation Challenges* (Stern School of Business, New York University, 2009)
17. A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S. Sadhukhan, *Cyber-risk decision models: To insure IT or not?* (Decision Support Systems, New York, 2013)
18. H. Ögűt, S. Raghunathan, N. Menon, *Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection* (Decision Support Systems, New York, 2011)
19. R. Böhme, G. Kataria, *Models and measures for correlation in cyber-insurance* (University of Logano, Logano, 2006)
20. J. J. Cebula, L. R. Young, *A taxonomy of operational cyber security risks* (Carnegie Mellon Univ, London, 2010)
21. G. Strupczewski, *Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie* (Czasopismo Komitetu Nauk o Finansach PAN, Krakow, 2017)
22. I. Kolechkina, I. Verchagina, E. Eltsova, M. Petrova, E3S Web Conf., **134**, 02004 (2019)