Risk Management of External Resources in Digital Ecosystems

Kari Koskinen
Aalto University
kari.m.koskinen@aalto.fi

Sonja Hyrynsalmi
LUT University
sonja.hyrynsalmi@lut.fi

Matti Rossi
Aalto University
matti.rossi@aalto.fi

Kari Smolander
LUT University
kari.smolander@lut.fi

Abstract

Participation in digital ecosystems entails the use of externally provided resources such as data, computing capabilities and digital functionalities. Though in many ways useful, these also create dependencies between organizations and pose them to risks that they have little direct control. The question that emerges is how to manage these type of ecosystem risks, which evolve from the digital dependencies created by the digital interconnections between ecosystem actors. By interviewing relevant personnel from companies participating to digital ecosystems and thus utilizing externally provided digital resources, the research evaluates to what extent existing risk management approaches can be utilized to address ecosystem risks. The research finds that risk management in ecosystems rests more upon rationalization than concrete actions to address risks. It further suggests more collective responses to managing ecosystem risks and, among others, highlights the use of alliances of ecosystem resource-takers to counter ecosystem risks.

Keywords: Risk, risk management, digital ecosystems, external resources, non-focal actors

1. Introduction

Information systems increasingly utilize externally provided digital resources and infrastructural services that require digital connections between otherwise separate systems and actors (Nambisan et al., 2017; Tilson et al., 2010). These resources are obtained via system integrations, which paves the way for the emergence of networks of connected systems that exchange computing capabilities, data and functionalities (Adner & Kapoor, 2010; Henfridsson & Bygstad, 2013). The digital connections and reliance on resources provided by others form the basis of digital ecosystems (Evans & Gawer, 2016; Um et al., 2015).

Ecosystems have been defined as *"the alignment structure of the multilateral set of partners that need to interact in order for a focal value proposition to materialize"* (Adner, 2017, p. 40). Crucial for these interactions in digital ecosystems are the technological connections, such as application programming interfaces (APIs), through which the different ecosystems actors and their systems are connected to one another (Monaghan et al., 2020; Parker et al., 2017). The interconnectedness of actors contributes towards ecosystem-wide modularity, which allows the formally interdependent actors of the ecosystem to coordinate their actions (Jacobides et al., 2018). In digital ecosystems, modularity surfaces in the ability for an actor to recombine the available digital resources into a variety of digital services and products (Gawer, 2014; Jacobides et al., 2018), reflecting the view of those as largely decentralized constellations of different actors without clearly established boundaries or hierarchies (Jacobides et al., 2018; Nambisan et al., 2017).

At the same time, resorting to resources managed and developed by others also creates technological dependencies between ecosystem actors (Öbrand et al., 2019). The dependencies become a source for IT-related risks, which may impact a system's development, maintenance and use (Dellermann, 2016). Any problem encountered by the provider of an external resource can spread to systems that are connected to the resource and rely on it in their functioning (Bresnahan & Greenstein, 2014). With externally provided resources, the user of the resource, i.e., the resource-taker, has limited influence on how the resource is managed and maintained. This type of setting is often found on innovation platforms, defined as *"foundations upon which other firms can build complementary products, services or technologies"* (Gawer, 2009, p. 54). Innovation platforms are seen as instances of digital ecosystems, characterized by the dependency of the complementors on the core platform, since the former relies on the boundary resources provided by the latter (Baldwin & Woodard, 2009; Ghazawneh & Henfridsson, 2013). The power balance between the two is often skewed towards core platform, which act as resource-providers (e.g. Eaton et al., 2015).

In essence, software artifacts that are developed and managed especially by smaller actors often rely on

URI: https://hdl.handle.net/10125/107147
978-0-9981331-7-1

multiple external resources, such as data, software libraries, functionalities, and computing capabilities (Fink et al., 2020; Um et al., 2015), provided by a multitude of digital platforms and other resource-providers. At the same time, even the bigger actors providing the resources are likely to use at least some external resources and expose themselves to similar risks. Due to the interconnectedness between various independent actors, all of them become subjected to a variety of risks posed by the externally provided resources via the technological dependencies those create. These risks call for risk management, yet in this setting it comes with a set of challenges since control over the system's functioning also resides to a variable degree outside the organization (Koskinen et al., 2021).

The question that emerges is then how exactly to manage and address these kinds of risks in digital ecosystems. This is of particular importance to the actors that act primarily as resource-takers in the ecosystems. Overall, these non-focal resource-takers have remained understudied in information systems research, and calls have been made to better understand their role for instance in platform ecosystems (McIntyre & Srinivasan, 2017; Selander et al., 2013). Our research seeks to contribute to this by investigating how resource-takers understand and manage risks that emerge from the dependencies that are inherent in digital ecosystems, and sets the following research question: *how do actors in an ecosystem manage risks that emerge from the use of externally provided digital resources?*

2. Risks and information systems

Risks have been described as the difference between possibility and reality (Renn, 1998) and are understood as negative outcomes that have a certain known or estimated level of occurrence (Willcocks & Margetts, 1994). Risks possess two key characteristics, namely likelihood of occurrence and impacts that follow from the occurrence (Misra, 2008). Due to their negative implications, risks require managing, defined as *"the identification of and response to potential problems with sufficient lead time to avoid a crisis"* (Pries-Heje et al., 2014, p. 62). Though risks vary, risk management is among the core activities of organizations.

2.1. Literature on information systems' risks

Djemame et al. (2016) view risks in organizations forming around an asset that is of value to an organization and therefore in need of protection against negative incidents. These incidents have the potential of impacting the asset's value or harm it in other ways. The harm or reduction in value leads to certain organizational losses, such as losses in revenues or business, company image, or share price (Salmela, 2008). Risk management is required to measure risks and assess their possible impacts ideally in quantifiable fashion, and based on that analysis, develop plans how to manage the risk or otherwise control the implications and impacts following the risks' occurrence.

An organization's information systems are considered as one significant source of organizational risks, already because information systems are vital for most organizational processes and functions and the cost of information systems related risk occurrence tends to be high (Willcocks & Margetts, 1994). Other organizational risks may also have a technological basis, such as in the case of risks emerging from technical uncertainty linked to experimenting with new technologies that the organization has no prior experience (Parker & Mobey, 2004).

The exact risk sources related to information systems have historically received a fair amount attention in information systems research (Öbrand et al., 2019). Risks have been mapped in various areas of information systems lifecycles, ranging from systems development to actual use of the systems. For instance, Lyytinen et al. (1996) saw that software-related risks generally emerged either in the development environment because of inexperienced developers, in the system environment due to inexperienced users, or more generally because of managers ignoring available information. Others have noted the importance of more technological factors such as system incompatibilities (Willcocks & Margetts, 1994). In addition, information that is processed and transferred in information systems can also be a source of risk. Westerman (2009) notes that these kinds of risks threaten organizations by hindering information availability, access, or accuracy.

Overall, research on information systems risk management has often produced checklists of project-level risks that need to be accounted for (Öbrand et al., 2019). Despite the occasional extensiveness of the checklists, it is difficult to include all possible risks, and it has also been seen challenging to know which risks are likely to be prevalent in each situation (Bannerman, 2008; Keil et al., 2008). To counter this, process models and situational approaches have been developed to assess risks and their resolution, describing a sequence of actions that needs to be taken to counter risks or noting the importance to study the specifics of each situation to exactly know, which risks are of relevance in a given situation and how to proceed in managing them (Persson et al., 2009).

Common to all these is that many of the identified information systems risks have largely emerged from within the organizational boundaries, to which the organization itself has much control over. However,

many of the information systems today cross organizational boundaries and are dependent on other systems and external infrastructure in their functioning, which often entails reduction of control over the factors that give rise to risk (Henfridsson & Bygstad, 2013). The key enablers of these kinds of risks are the interconnections that exist within and between systems, which also characterize and mediate participations in digital ecosystems.

The digitally enabled connections between systems are established, for instance, via APIs, which form the cornerstone of the functioning of most digital platforms and ecosystems (Pujadas et al., 2020). With the emergence of various digital platforms and ecosystems to which organizations seek to join, the systems have become more polycentric (Constantinides & Barrett, 2015). As the number of integrations and dependencies to other systems grows, the less control the owner of a specific information systems has over the whole (Öbrand & Holmström, 2013). In terms of risks, this implies a shift in risk management from internally focused actions towards policies that account for external actors that exercise significant control as owners of the resources that the internally managed systems depend on.

In research on strategic alliances and external outsourcing, risks controlled by external actors are common. Amiruddin et al. (2013) note that risks emerge in this context from areas such as cooperation between parties and meeting intended objectives. To manage these risks, the primary tools include establishment of formal (rules, procedures, and policies) and informal (norms, values and culture) control mechanisms (Amiruddin et al., 2013; Langfield-Smith, 2008).

However, risk management in ecosystem is likely to differ from that of outsourcing. To begin with, though formal rules and mechanisms are quite common in digital ecosystems, they are largely dictated by the resource-provider. In addition, the applicability of informal control measures is less clear as the relationships between resource-providers and takers are often that of arm's length (Ghazawneh & Henfridsson, 2013), established by ticking a checkbox confirming terms and conditions that consist of relatively standardized items with little room for modifications.

2.1. Approaches to managing risks emerging from the use of external resources

Risk management of identified risks often adopts one or several of the four commonly known risk management approaches. These four approaches or risk management strategies are risk avoidance, transfer, mitigation and/or acceptance (Djemame et al., 2016; Hillson, 2002). The first one, risk avoidance, seeks to eliminate the risk by either making it impossible to occur or reducing the risk's impact following its occurrence ideally to zero. Risk transfer enables actors to externalize risks or their negative implications to other organizations such as insurance companies or regulators (Mitev, 2011). Risks can be mitigated by reducing the impact or risk probability to levels that are deemed acceptable. Risk mitigation thus focuses on the two components of risk, impact, and likelihood, and aims to reduce either of those or both. Finally, risks can be accepted as they are, in which case they are seen as either necessary to take or that their impact or likelihood is low. Risk acceptance is present in all the risk approaches, since even after responses such as risk mitigation some residual risk often remains. Risk acceptance may also contain risk monitoring, so that the owners of the risk are the very least aware if the risk occurs and begin actions to address the impacts of the risk occurrence (Baskerville et al., 2008; Hillson, 2002).

When placed in the context of digital ecosystems, different risk response approaches are subjected to challenges that are less present in other kinds of operating environments. Risk avoidance, for instance, may simply not be possible due to the limited resources that many resource-takers possess, and there is no alternative for the utilization of externally provided resources. Risk transfer is likely to be more problematic in situations, in which sought value is difficult to assess. This is often the case with information or specific functionalities that cannot be treated as physical entities in a meaningful sense (Gerber & von Solms, 2005). Safe-guarding or self-insuring may take place though via contractual agreements regarding service level thresholds, but the negotiation of these thresholds is often better mastered by the resource-provider than the resource-taker (Salmela, 2008).

Risk mitigation contains its own challenges as the system owner may not have direct control over the resources the system requires. Risk mitigation calls for active measures to counter risk prior its occurrence (Moeini & Rivard, 2019). In information systems projects, risk mitigation traditionally occurs via user involvement, communication, requirement specification, and resource planning (Pries-Heje et al., 2014). However, risk mitigation in ecosystems can be more difficult to conduct if the resource and its control resides outside the organization. Risk mitigation strategies such as contingency planning have not always been seen as effective either (Brookfield et al., 2014) and can be difficult in this kind of setting. Finally, risk elimination can be challenging if a resource is crucial for a system to function, especially if no alternative providers for the resource exist (Koskinen et al., 2021). At the same time, risk acceptance can be costly too if the risks materialize.

Partly due to these difficulties, calls have been made for a more holistic approach for assessing especially IT risk that accounts for the openness and interconnections to other, often external, systems and the dependencies emerging from that (Gerber & von Solms, 2005).

3. Methodology

The data was collected during May 2021 – March 2022 and consisted of 20 interviews in total. As shown in Table 1, the interviewees were IT managers or related IT professionals such as system architects in different Finnish companies. The selection criteria for the interviewees were that the company's own systems and offerings depended on the use of external resources and the interviewee had a role in either managing or developing the system. In addition, we sought to identify interviewees who had substantial experience in working on the system's development or operations, so that they could also reflect upon their own experiences in terms of addressing risks emerging from the use of external resources.

All of the selected companies had systems, which were relying on one or more external resources. The most common of these were the use of public cloud services such as Amazon Web Services or Microsoft Azure. In addition to these, many of the companies also utilized other externally provided resources and tools such as cloud-based integration platforms or ticket booking systems or had built mobile applications to enable access to their own services, thus forming part of Apple's or Android's ecosystems. In some cases, the companies' systems were also reliant on data sources that were located outside the organizations. The relevance for this research emerged from the fact that by utilizing these resources, the companies either participated directly in the ecosystems, for instance, by creating complementarities, or found themselves in a position typical of that of ecosystem participation by being dependent on the resources provided and maintained by others.

The interviews were made in Finnish and conducted online due to the Covid-19 pandemic. The interviews were semi-structured and lasted from 60 to 90 minutes. In the interviews, the interviewers first mapped the ecosystems that the companies of the interviewees were part of, as well as inquired of any other external resources that the companies' systems were dependent on in their functioning. After this, the interview questions focused on the perception of risks by the interviewees regarding the use of external resources, and then inquired about the concrete risk management actions that had been taken in the companies to address the risks. The interviews were recorded, transcribed, and coded using Atlas.ti.

ID	Title	Company size	Interview length (min)
i1	CIO	20-49	62
i2	CIO	1000-2499	50
i3	Architect	2500-4999	75
i4	Manager	5000-9999	47
i5	CIO	100-249	41
i6	Manager	250-499	51
i7	Architect	2500-4999	41
i8	Director	500-999	47
i9	CDO	500-999	47
i10	Manager	250-499	65
i11	Architect	250-499	57
i12	Manager	1000-2499	54
i13	Architect	10000-19999	58
i14	Manager	100-249	64
i15	CIO	1000-2499	49
i16	CIO	5000-9999	41
i17	CIO	20000-39999	52
i18	CIO	100-249	44
i19	CIO	20-49	51
i20	CEO	20-49	51

Table 1. List of interviewees

The data were analyzed by using thematic analysis, which was guided by first understanding the perception of risks by the interviewees and then the different risk management approaches utilized by the companies to address these kinds of risks. Particularly the interest was in seeing which risk management actions could be categorized under each of the approaches. The coding did also leave room for other approaches to emerge from the data in case interviewees discussed measures to address risks that did not entirely fit with any of the four risk management approaches. The results of the analysis enabled the authors to identify similarities in the responses of the different interviewees, which allowed the authors to conclude that the key aspects regarding managing risks emerging from the use of external resources had been covered in the conducted interviews.

4. Findings

4.1. Risk awareness

The findings show that the interviewees were aware that participation in digital ecosystems came with risks. Systems were seen as becoming more complex and the interconnections between systems increasing.

"I am not saying that it used to be better or that I would miss the past, but it was easier to understand and know what the situation was at each moment." (i11)

"For the past 20 years, the use of different libraries and information technology has led to higher level of abstraction, and those libraries on their part are dependent on other libraries, and that pile just keeps on growing" (i3)

It was acknowledged that it is not possible to even be aware of everything that occurs in these systems:

"Things we have encountered include server downtime that has gone unnoticed, or some human errors that have led to bigger problems. We just had an incident of which no error notification was triggered, and we did not realize it or the gravity of its implications." (i4)

Though it was also stated that tools to track errors and monitor systems had improved, the external resources were often at least partially black-boxed or opaque, which also meant that it was difficult to know exactly in error situations what had happened in the externally provided resources. Similar challenges arose in terms of system updates, as a change in the external resource occasionally impacted the functioning of the resource-taker's system.

"When you have any kind of cloud service that is updated, you have no control over the update but just need to make sure your system still works [..] the promise is that this would not happen, but there is always an upgrade to the current version and as a result, the very least you have to test your systems" (i15)

The importance of following set guidelines and rules was overall raised in the interviewees as a prerequisite for a successful ecosystem:

"If we are running an integration platform, and communicated to our partners that this is the maximum amount [of data] the platform has been designed to and what we cannot exceed. So if someone opens the floodgates upstream, there is nothing we can do (i17)

In terms of infrastructure, new risks emerged in terms of network connectivity.

"As we are in the cloud, the network connectivity has to be designed in a manner that our most critical functions work even if we end up being offline. And the more cloud-native services we are building, the more difficult this becomes" (i11)

The relative power positions were also seen as a possible risk. If power disparity between resource-takers and providers was large enough, the former had little influence on the resources they purchased or otherwise obtained. Contracts between parties were often offered in the form of 'take it or leave it' with little room for negotiating any customized deviations from the established terms or conditions.

"People always ask us how often we keep SLA-meetings with our cloud service provider, we do not even have those since we do not spend enough money, even though in the Finnish context we are quite a big actor. This also means that we have to make contingency plans if any kinds of events that are unrelated to us would occur […] if something did happen, we are talking about recovery time of weeks, even months." (i18)

Use of external resources such as data, computing capabilities or software libraries created risks for the resource-takers. Many reminded though that the use of purely internal resources was not without risks either. It was also seen that the bigger actors had more resources to address risks and unlikely to do anything that would go against the interests of their key clients. However, none of these factors helped the actors to obtain any control over the provided resources.

4.2. Risk avoidance

Prior to resource adoption, risk avoidance could be practiced by simply avoiding external resources that were deemed of containing too much risk or riskier than similar resources provided by other external actors. Trials and testing before adopting a resource were used to establish the functioning and fit of the resource and to assess the risk it posed to the organization.

"With trials you can make things more concrete, you make sure things work by having a trial period or other verification instead of just believing PowerPoints and others. That way you also become familiar with the issues that otherwise are facing you after the adoption and you know to ask the questions after the trial." (i11)

It was recognized that the resource-taker had limited options to counter the resource-provider after the resource was taken into use. Switching from one resource-provider to another was an option to avoid risks when they emerged, yet often this also presented its own set of challenges.

"Once a contract has been made [with a resource-provider], you are married with those contracts. […] how much risk of ending up arguing with the resource-provider you are willing to accept […] they [the resource-provider] can press the button to stop your systems from working as a last resort to get their way" (i5)

Another option to avoid risks related to externally provided resources was to obtain those from different sources or to have duplicate systems in place. However, this also meant additional costs.

"Whether to duplicate or triplicate a particular piece of your system architecture is a matter of cost, and well, not everything can be done" (i20)

Finally, another clear example of avoiding risks emerging from the utilization of external resources was to own the resources and control those in-house. Occasionally at least the most critical parts of a system were maintained and managed on-premise.

"A large part of our systems are still kept here as on-premise solutions, and we even host a closed information network regarding those systems. […] At the same time, other parts of the system are ran on the cloud, so we had to have a system that enabled to run part of the process there and then jump back to our own [on-premise] systems" (i19)

Overall, it was widely seen that avoiding risks resulting from external resources was costly, difficult at best, or simply not even feasible.

4.3. Risk transfer

When resources were adopted from external providers, this could be also seen as an instance of risk transfer. For instance, if hardware resources were provided by an external actor such as cloud service provider, it could be seen that in the same process risks were also transferred to the provider, such as those related to security. However, risks could not be transferred in their entirety, but a proportion of it remained with the resource-taker.

"Transferring it [risk] is very difficult, bigger actors and all those SLAs, they do not compensate for the cost that is incurred" (i9)

"It is more about risk sharing, the providers are not willing to remove all the risk from us, they always want to make sure they make profit too so the risk always stays with us" (i6)

Even though the risks could not be transferred entirely to the resource-provider, adopting external resources did mean that the control of the resource and with that a large part of risk management was transferred to the resource-provider. The risk assessment done by the resource-taker thus focused on the perceived ability of the resource-provider to manage the risk. The stated assumption was often that bigger the resource provide was, the better they were able to do this.

"If it was some smaller provider, they [customers to an organization] might be angrier and demand more [compensation], but they don't necessarily do that for a bigger actor like Microsoft. In a way, it is about being powerless when dealing with such massive companies" (i16)

While a large share of active risk management was thus transferred to the resource-provider, there was less to protect resource-takers from reputational damage if there were problems with the adopted resource.

"There is no point us telling [to our customers] that the problem is in [the external system], we just try to get them [the resource-providers] to fix the problem as quickly as possible. We take the blame and that is why we also need to have as good contracts as possible with the resource-provider, as well as good cooperation to get the problems fixed" (i4)

However, there was some indication that in terms of risk transfer, bigger actors were possibly a better solution as they were often seen as having the resources to better manage the risks. In a similar vein, as number of actors were adopting resources from the same source, the risks became shared by many, which also meant that if one actor faced problems with the adopted resource, others were possibly encountering the same problem.

"If we have a problem with Salesforce or Azure, usually the implications are larger than that of just our company. If you can say that it is because of this reason, it is usually easier, though then you do have to also think how long can your business survive without the resource, and if it is some smaller actor, it will take longer to get things back on track again" (i5)

Generally, the bigger actors were seen as more trustworthy in terms of risk management, and hence, even though risks could not be transferred entirely, they were seen in better care and managed by the major resource-providers, also in comparison to the resource-taker itself.

"Because the maintenance of systems is in so much better level [with the bigger resource-providers], there is not much one has to worry about. Were you to build something similar on-premise, that does not sound very appealing at least to me" (i12)

In essence, use of an external resource transferred an active part of the risk management to the resource-provider. However, it did not allow the resource-takers to get rid of the risk completely as, for instance, reputational risk remained with the resource-taker.

4.4. Risk mitigation

If risks related to adopting external resources could not be avoided nor entirely transferred to the resource-provider, the actors adopting resources had the option of mitigating risks. Several factors such as system transparency contributed towards resource-takers' ability to mitigation risks related to external resources.

"[The utilized resource] allows now for greater transparency. It has been difficult in the past, with

tickets flying around, if something did not go from point A to point B, I first blamed A and then B, and finally C. Each one of those does send a bill, but the solution to the problem is not easy to find" (i15)

This transparency was of importance since monitoring was seen as a vital component of risk mitigation of external resources. Monitoring gave the actors a possibility to source any errors or problems quickly, which helped to address any implications of risk occurrence.

The ability to monitor the various parts of a system, including external resources, contributed thus to the ability to react quickly if something failed. The least preferable option that was cited by one interviewee was if the customer had to note the system owners of any errors occurring in the system. Monitoring was therefore also connected to back-up planning, i.e., having clear processes in place instructing what to do if a particular error occurred, which formed another area for risk mitigation.

In addition to these, availability and level of support was often brought up in the interviews. While it was emphasized that the availability of support had to establish before adopting a resource, it was also noted that especially when dealing with bigger actors, high level of support came with a cost.

"If you are not willing to pay, well, I think quite a few resort to the thinking that hopefully everything works as the resource-provider is a big company. Then if there are big problems [with the resource], then there is no point shouting them to fix the issue, everyone else [of actors using the resource] is in the same mess and it is not that easy for the bigger actors either to always solve the errors." (i9)

At the same time, not being too dependent on one resource-provider was also seen as mitigating risks.

"Currently Microsoft is probably the only one that has a real stronghold on us. Regarding other areas, we have actively tried to avoid situations that we could not switch to another or to impact them [the resource-provider]" (i2)

While the above were more reactive measures to mitigate risks and their impacts, there were also some actions that could be taken prior the risk had occurred. For instance, system insulation limited the negative impacts a risk occurrence might have.

"We aim to insulate these systems from one another, so that if there is a service break in one part of the system, the other system is aware of this and only continues sending the messages once the other system is back in operation." (i17)

Similarly, preparation in terms of conducting auditing checks as well as generally making sure that a company's own security measures were at a sufficient level were also mentioned as risk mitigation. The interviewees also saw that using external resources could in itself be seen as a form of risk mitigation, given that those were provided by a reputable actor.

Finally, when plausible, forming alliances with other users of the same resource was considered a good practice to have more influence on the resource-provider.

"Our closest partner that has a similar structure and uses the same system is in New Zealand. […] By joining forces and making joint requests we can add a bit more weight to those requests." (i11)

The partnerships were not to be seen merely as a counterforce to the resource-providers, but occasionally the resource-providers actively supported the cooperation between resource-takers.

"The [resource-provider] has this kind of community platform with voting functionality, so each actor can suggest changes and has a share of votes based on their size to vote whether to go ahead with the new functionality or not […] you can also become nominated as a champion regarding a product that is developed, and in that case you have more say on how that product is going to be developed" (i4)

Cooperation enabled the resource-takers to have more say in how the resource was being developed. Though this did not translate into direct control over the resource-provider, it did give them power to address risks and enabled the resource-taker to have a more active role in deciding how to approach identified risks.

4.5. Risk acceptance

Risks were occasionally simply accepted. Among the reasons for accepting risks was, for example, that the risk likelihood seen as particularly low. Resorting to resources provided by bigger actors were seen as less risky and hence easier to accept without specific risk management actions.

"Surely one prefers to store one's money in a [bigger bank] than to a hat of a local businessman. These bigger companies have a certain reputation they want to protect. And even though you do face these unpleasant situations that the terms and conditions are being changed and more money is being spent, none of them is that stupid that they would mess with data leaks or cybersecurity or usability, so it is safer in that sense." (i2)

Compared to the past, some interviewees also pointed out that by simply adopting externally provided resources reduced some of the risks, which also contributed to the approach of simply accepting those.

"Of course, we think of whether to accept the residual risk that exists […], but one also needs to have a holistic view so that even though if the solution is not

perfect, it might still better to how things were before." (i2)

Though the risk itself was accepted, risk mitigation could still occur in terms of preparing for the situation followed by the risk occurring

"We need to be able to access support services 24/7, as well as good monitoring capabilities including appropriate logs, so we can react to the problem as quickly as possible and solve it." (i4)

In conclusion, the different risk management approaches all surfaced in the interviews and concrete examples were given how each of the approaches could be adapted to address the risks emerging from the use of external resources. At the same time, none of the approaches helped to fully counter the loss of control from the resource-taker to the resource-provider.

5. Discussion and conclusion

The different risk management approaches and their contents are summarized in Figure 1.

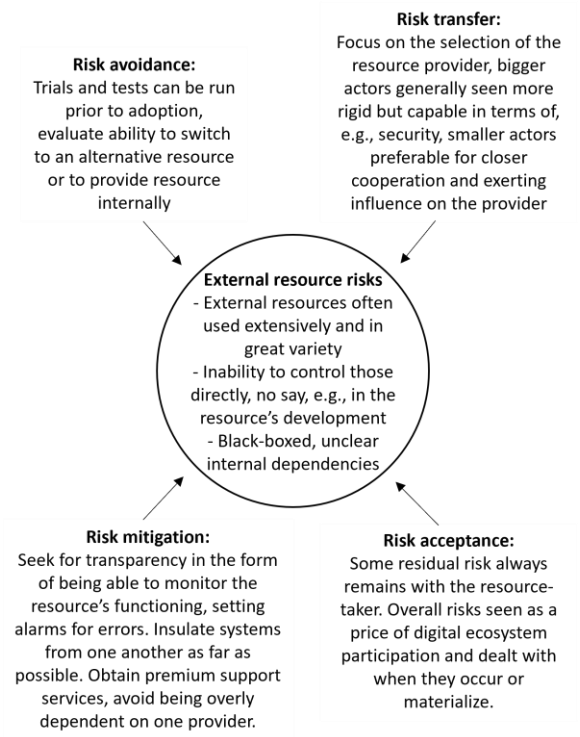

Figure 1. Risk management of external resources

Resource-takers can apply different risk management approaches, though most of those are focused either on the phase preceding resource adoption or on actions done once the risk has materialized. Risk management actions that can be exercised during the use of the resource are more limited. Since the resource-takers are not typically involved in the decision-making processes concerning the resource, they have little say on its development or maintenance, nor do they have direct access to the resource itself as that is solely managed by its provider. This also means that the internal dependencies of a resource, for instance, to which other external resources the obtained resource itself relies on, are not necessarily known for the resource-taker. At the same time, as more and more of actors take part in different digital ecosystems, these external resources are increasingly used in organizations and vary in their shape and purpose.

5.1. Theoretical implications

Much of the risk management of external resources after the resource adoption is not proactive but reactive by its nature. It also heavily relies on resource-providers' support services. This also challenges the views of seeing risks emerging from organizational assets (Djemame et al., 2016), as the asset resides outside the organization. While this does not change the nature of the risks as influencing organizations, for example by imposing costs (Willcocks & Margetts, 1994) or threatening the accuracy or availability of information (Westerman, 2009), these differ from traditional IS risks due to their externality and lack of control by the resource-taker. What follows is that these kinds of risks can only be partially addressed by using checklists (Schmidt et al., 2001) and are less dependent on factors such as employees' skills or managers' incompetence (Lyytinen et al., 1996). Similarly, factors like system incompatibilities that pose risks to a particular system (Willcocks & Margetts, 1994) may reside fully outside the organization. At the same time, differences in power balances that favor the resource-providers over the resource-takers, lessons from strategic alliances or external outsourcing (Amiruddin et al., 2013) are not directly applicable either.

Instead, risk management in digital ecosystems seems to rely more on rationalizations and logical reasonings rather than concrete actions. These are a form of risk acceptance and rest upon three, partially related, premises. First, the thinking is that even though these external ecosystem risks cannot be properly controlled due to their externality, the overall situation does not significantly alter or is even better when compared to having the required resources in-house. In other words, it is not that internal resources and having direct control over the resources is a risk-free exercise either. Second, the resource-providers are seen better equipped to deal with the risks as they have the expertise regarding the resource. Especially if the resource-provider is bigger, it is assumed to have the capabilities and motivation to make sure that everything works as expected. Thirdly, a resource-taker uses the

rationalization that everything should work as intended as long as the interests of resource- providers are aligned with theirs. Most often this is the assumed state of affairs, and the resource-provider seen as unlikely to act in a manner that is harmful for the resource-taker.

Irrespective of the apparent soundness of the three premises, risks have materialized in digital ecosystems with occasionally grave implications for the resource-takers. In addition, resource-providers do not always act in the best interest of resource-takers. The bigger the resource-provider is, less say the resource-taker has. At the same time, bigger resource-providers are seen as a safer and more trustworthy option, since they are likely to possess more capacities to deal with risks. In addition, the consequences of a risk materializing are shared with other users of the resource, which might increase the urgency of fixing issues. A certain risk related network effect is in place that favors the bigger actors over the smaller ones: more customers a platform has, the more reason and more resources it has for risk management. This again functions as an incentive for other customers to join. Smaller resource-providers are generally seen as more flexible though and allowing creative solutions. They are viewed as more open to different forms of cooperation, which also offers the resource-takers more proactive actions for dealing with these kinds of risks.

Overall, risk management of externally provided digital resources appears to contain various trade-offs. While resource-takers are aware of the challenges and risks linked to external resources, they deem those acceptable as at least momentarily the benefits seem to be greater. There is a need to better understand what types of trade-offs resource-takers are willing to accept as well as what kinds of combinations of risk management approaches to use to address these risks.

5.2. Practical implications

The power balance between resource-providers and -takers can be made more equal by the establishment of alliances between resource-takers. These alliances may increase their influence over the resource-provider and push, e.g., for changes in the resource or demand for more transparency on resource maintenance and operations. The resource-providers may even facilitate the formation of these alliances, though the success of the alliances is conditioned by resource-provider's size.

Risk management in digital ecosystems that relies on the actions of individual actors alone is unlikely to provide the best results. A more collective approach through alliances shows how individual resource-takers can have a more active role in risk management as the alliances provide possibilities for more proactive risk management actions or may enable the resource-takers to keep resource-providers more accountable. However, the alliances would need to be extremely big to counter the major resource-providers of digital ecosystems.

6. Acknowledgements

This research was funded by Research Council of Finland, project #328737: Strategic approach to scalable platform based software and systems development.

7. References

Adner, R. (2017). Ecosystem as Structure: An Actionable Construct for Strategy. Journal of Management, 43(1), 39–58.

Adner, R., & Kapoor, R. (2010). Value creation in innovation ecosystems: How the structure of technological interdependence affects firm performance in new technology generations. Strategic Management Journal, 31(3), 306–333.

Amiruddin, R., Aman, A., Auzair, S. M., Hamzah, N., & Maelah, R. (2013). Mitigating risks in a shared service relationship: The case of a Malaysian bank. Qualitative Research in Accounting & Management, 10(1), 78–93.

Baldwin, C. Y., & Woodard, C. J. (2009). The Architecture of Platforms: A Unified View. In A. Gawer (Ed.), Platforms, Markets and Innovation. Edward Elgar Publishing.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. Journal of Systems and Software, 81(12), 2118–2133.

Baskerville, R., Straub, D., & Goodman, S. (2008). Strategic information security risk management. Information Security Policy, Processes, and Practices, 112–122.

Bresnahan, T., & Greenstein, S. (2014). Mobile Computing: The Next Platform Rivalry. The American Economic Review, 104(5), 475–480.

Brookfield, D., Fischbacher-Smith, D., Mohd-Rahim, F., & Boussabaine, H. (2014). Conceptualising and responding to risk in IT projects. Risk Management, 16, 195–230.

Constantinides, P., & Barrett, M. (2015). Information infrastructure development and governance as collective action. Information Systems Research, 26(1), 40–56.

Dellermann, D. (2016). The Thrill and the Agony of Digital Ecosystems: A Complementor\' s Perspective on Co-Innovation Risk. The 10th Ratio Colloquium for Young Social Scientists, Organizing for Digitalization, Stockholm.

Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2016). A Risk Assessment Framework for Cloud Computing. IEEE Transactions on Cloud Computing, 4(3), 265–278.

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2015). Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System. MIS Quarterly, 39(1), 217–243.

Evans, P., & Gawer, A. (2016). The Rise of the Platform Enterprise: A Global Survey (1; The Emerging Platform Economy Series). The Center for Global Enterprise.

Fink, L., Shao, J., Lichtenstein, Y., & Haefliger, S. (2020). The ownership of digital infrastructure: Exploring the deployment of software libraries in a digital innovation cluster. Journal of Information Technology, 35(3), 251–269.

Gawer, A. (Ed.). (2009). Platforms, Markets and Innovation. Edward Elgar Publishing.

Gawer, A. (2014). Bridging differing perspectives on technological platforms: Toward an integrative framework. Research Policy, 43(7), 1239–1249.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. Computers & Security, 24(1), 16–30.

Ghazawneh, A., & Henfridsson, O. (2013). Balancing Platform Control and External Contribution in Third-Party Development: The Boundary Resources Model. Information Systems Journal, 23(2), 173–192.

Henfridsson, O., & Bygstad, B. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. MIS Quarterly, 37(3), 907-A5.

Hillson, D. (2002). Extending the risk process to manage opportunities. International Journal of Project Management, 20(3), 235–240.

Jacobides, M., Cennamo, C., & Gawer, A. (2018). Towards a Theory of Ecosystems. Strategic Management Journal, 39(8), 2255–2276.

Keil, M., Li, L., Mathiassen, L., & Zheng, G. (2008). The influence of checklists and roles on software practitioner risk perception and decision-making. Journal of Systems and Software, 81(6), 908–919.

Koskinen, K., Hyrynsalmi, S., Rossi, M., & Smolander, K. (2021). Quest for Control: Managing Software Development in Networked Operating Environments. In Proceedings of the 54th Hawaii International Conference on System Sciences, 5965–5974.

Langfield-Smith, K. (2008). The relations between transactional characteristics, trust and risk in the start-up phase of a collaborative alliance. Management Accounting Research, 19(4), 344–364.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1996). A Framework for Software Risk Management. Journal of Information Technology, 11(4), 275–285.

McIntyre, D. P., & Srinivasan, A. (2017). Networks, platforms, and strategy: Emerging views and next steps. Strategic Management Journal, 38(1), 141–160.

Misra, K. B. (2008). Risk analysis and management: An introduction. Handbook of Performability Engineering, 667–681.

Mitev, N. (2011). Beyond health warnings: Risk, regulation, failure and the paradoxes of risk management. Journal of Information Technology, 26(4), 271–273.

Moeini, M., & Rivard, S. (2019). Sublating Tensions in the IT Project Risk Management Literature: A Model of the Relative Performance of Intuition and Deliberate Analysis for Risk Assessment. Journal of the Association for Information Systems, 20(3).

Monaghan, S., Tippmann, E., & Coviello, N. (2020). Born digitals: Thoughts on their internationalization and a research agenda. Journal of International Business Studies, 51(1), 11–22.

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital Innovation Management: Reinventing Innovation Management Research in a Digital World. Management Information Systems Quarterly, 41(1), 223–238.

Öbrand, L., Augustsson, N.-P., Mathiassen, L., & Holmström, J. (2019). The interstitiality of IT risk: An inquiry into information systems development practices. Information Systems Journal, 29(1), 97–118.

Öbrand, L., & Holmström, J. (2013). Recalcitrant technologies and unfolding ontologies: Exploring the emergent character of IT risks and epistemic strategies in IT risk management. The 29th European Group for Organization Studies (EGOS) Colloquium, Montreal, July 4-6, 2013.

Parker, D., & Mobey, A. (2004). Action research to explore perceptions of risk in project management. International Journal of Productivity and Performance Management, 53(1), 18–32.

Parker, G., Van Alstyne, M., & Jiang, X. (2017). Platform Ecosystems: How Developers Invert the Firm. MIS Quarterly, 41(1), 255–266.

Persson, J. S., Mathiassen, L., Boeg, J., Madsen, T. S., & Steinson, F. (2009). Managing risks in distributed software projects: An integrative framework. IEEE Transactions on Engineering Management, 56(3), 508–532.

Pries-Heje, J., Venable, J., & Baskerville, R. (2014). RMF4DSR: A Risk Management Framework for Design Science Research. Scandinavian Journal of Information Systems, 26(1), 57–82.

Pujadas, R., Valderrama, E., & Venters, W. (2020). Interfaces and the Dynamics of Digital Ecosystems: A Study of the Online Travel Ecosystem. ICIS 2020 Proceedings.

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. Journal of Risk Research, 1(1), 49–71.

Salmela, H. (2008). Analysing business losses caused by information systems risk: A business process analysis approach. Journal of Information Technology, 23(3), 185–202.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. Journal of Management Information Systems, 17(4), 5–36.

Selander, L., Henfridsson, O., & Svahn, F. (2013). Capability Search and Redeem across Digital Ecosystems: Journal of Information Technology, 28(3), 183–197.

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research Commentary—Digital Infrastructures: The Missing IS Research Agenda. Information Systems Research, 21(4), 748–759.

Um, S., Yoo, Y., & Wattal, S. (2015). The Evolution of Digital Ecosystems: A Case of WordPress from 2004 to 2014. ICIS 2015 Proceedings.

Westerman, G. (2009). It Risk as a Language for Alignment. MIS Quarterly Executive, 8(3), 109–121.

Willcocks, L., & Margetts, H. (1994). Risk assessment and information systems. European Journal of Information Systems, 3(2), 127–138.