When is IT Unavailability a Strategic Risk?: A Study in the Context of Cloud Computing

Research-in-Progress

Amin Khodabandeh Amiri
amin.amiri@sauder.ubc.ca

Hasan Cavusoglu
cavusoglu@sauder.ubc.ca

Izak Benbasat
benbasat@sauder.ubc.ca

Sauder School of Business,
The University of British Columbia,
2053 Main Mall,
Vancouver, BC V6T 1Z2 CANADA

Abstract

As organizations are becoming increasingly dependent on Information Technologies (IT) to run their business processes, they are also becoming more susceptible to its discontinuity. Anecdotal evidence exists for many cases of IT service interruption that resulted in strategic consequences such as financial losses, negative stock market reactions, reputational damages or even organizations' existence. However, not all IT Unavailability incidents have caused strategic losses. This research-in-progress paper proposes a model to help understand when an IT unavailability risk is a strategic risk and in need of special attention by board members and senior executives. A survey is proposed to be conducted to examine the validity of the model in the Cloud Computing context.

Keywords: IT Unavailability, Strategic Risk, Capability, Alignment

Introduction

Information Technology Risk, which is “the potential for an unplanned event involving Information Technology (IT) to threaten an enterprise objective”¹ (Westerman & Hunter, 2007, p. 22), has been attracting more organizational attention (Goldstein et al., 2011). This is often because organizations rely increasingly more on IT (Vitale, 1986). As such, the risk of interruption in IT services, IT Unavailability Risk hereafter, is one of the most critical IT risks that organizations face. For example, an hour downtime of operation would cost Amazon $180,000, eBay $225,000, and an airline reservation center $89,000 (Patterson, 2002). Comair’s crew-scheduling system failure during the holiday season in 2004 caused millions of dollars losses and led to the resignation of Comair’s president (Westerman, 2009). A poll conducted by ABC News and Washington Post (Post-ABC poll, 2013) right after Obamacare’s website shutdown showed that President Obama could have lost his second term of presidency to his opponent if the election had been right then. There is no shortage of scary, real-world stories of IT disruptions in which IT systems’ unavailability resulted in significant losses or strategic consequences (Chen et al., 2011).

¹ There is a lack of consensus among IS researchers on the definition of IT risk. One aspect of this disagreement is whether IT risk should focus exclusively on negative outcomes or it could include both threats and opportunities (Alter & Sherer, 2004; Benaroch et al, 2006). This study adopts the former focus.
On the other hand, so many system interruptions have not resulted in any noticeable trouble for organizations at the strategic level. Dynes et al. (2007) has found that information system disruptions within supply chain of an electrical component manufacturer would not affect the firm’s strategic ability to manufacture parts. Likewise, Novartis’ CIO argued “It probably doesn’t matter if one of our payroll systems breaks. We can give people cash; we’ll give them checks. It’s no business risk whatsoever” (Westerman & Hunter, 2007, p. 21). Similarly, there is also no shortage of real-world stories of IT service disruption in which systems’ unavailability did not result in noticeable financial loss or strategic consequences.

This raises important question of which and under what conditions IT disruptions are strategic risks and hence require the attention from top executives and board members. It is worthwhile to note that managing strategic risks has become a growing concern for both boards and top executives (Drew et al., 2006). Such trend could be attributable to the fact that negligence of strategic risk can quickly result in a loss of competitive edge (Drew et al., 2006) or to the regulatory requirements such as Sarbanes— Oxley Act of 2002 (Bai et al., 2013; Drew et al., 2006). Therefore, it is conceivable that CEOs and board members want to know the sources of strategic risks rooted in each functional area, including IT. Yet, no proper framework or approach exists to help managers identify strategic risks (Parent & Reich, 2009). The purpose of this paper is to expand our understanding of strategic IT risk by answering when IT unavailability is a strategic risk.

This paper is organized as follows: the next section provides the research model and the theoretical development based on the literature of Strategic Management and Information Systems. Then, the research methodology will be discussed. Finally, the paper concludes with a discussion of desirable findings.

**Research Model and Theoretical Development**

The research model developed to answer our research question is anchored on business capability. A business capability is what a business does, but not how it is implemented in terms of people, procedures, resources, and technology. We have business capability perspective for two reasons. First, capability is a concept which is easily understood by CEOs and Board members as well as IT practitioners. Thus, it can facilitate communications of IT Risks between business and IT (Ulrich & Rosen, 2011). Second, capabilities are relatively more stable and thus yield a relatively longer-lasting model of the area of focus (Homann, 2006) which makes them suitable to serve as a baseline for strategic management and impact analysis (Ulrich & Rosen, 2011). Our research model is presented in Figure 1, followed by development of hypotheses based on the literature of Strategic Management and Information Systems.

---

1 This study assumes that all types of IT Unavailability such as hardware outage, network disruption, or data unavailability demonstrate themselves through application unavailability (see Zambon et al., 2007) which business really cares about. As this study views IT risk from business perspective, IT Unavailability is meant to refer to Application Unavailability. In addition, the scope of our study includes applications that are at the stage of operation and maintenance (not at investment decision, development, and legacy stages) in the IS life cycle.

2 A criticism that might be made in relation to this question is that practitioners and managers are quite good at figuring out IT disruptions which are potentially strategic. We have interviewed six IT practitioners and also solicited feedback from professional discussion group formed in LinkedIn on IT governance and risk and received answers from seven practitioners. Based on interviews and the forum post, it appears that practitioners engaged do not have a good method to determine the strategic impact of an IT unavailability. Only two out of thirteen practitioners were able to provide a scenario under which IT Unavailability could cause strategic. Those two took business processes perspective which we reasoned against in the paper where we advocate capability perspective. Therefore, it seems that practitioners and managers may not be as good at determining which IT disruptions are strategic as one might have thought.
When is IT Unavailability a Strategic Risk?

Strategic Risk

The significance of strategic risk has not led to a consensus on its definition in the literature. Strategic Management literature has more focused on covariance or variance-based definitions (e.g., variance of Return on Investment) (Ruefli et al., 1999) that do not consider the relative nature of strategic risk (Collin & Ruefli, 1992). The current study takes Collin & Ruefli’s (1992) approach and defines Strategic Risk as the probability of losing rank position in the set of firms that are producing products or services that are close substitutes for each other. Therefore, a phenomenon is a strategic risk if it threatens a firm’s long-term competitive position and survival (Drew et al., 2006). Such outcomes can be materialized in the form of losses of market share (Tanriverdi et al., 2007; Drew et al., 2006), financial health (Tanriverdi et al., 2007), critical resources, ability to innovate and grow (Drew et al., 2006), ability to react flexibly to changes in the market, and the know-how that will be required to remain competitive in future markets (Gewald & Dibbern, 2009).

As mentioned above, IT resource weaknesses, such as IT Unavailability, can cause competitive disadvantage for firms and result in a decrease in market valuation (Goldstein et al., 2011). However, to answer the question of when the impact of IT Unavailability is strategic, we need to review the IS literature on IT unavailability assessment.

Business Impact Analysis (BIA) of IT Unavailability

IT availability risk assessment is generally influenced by three factors (Liu et al., 2010): likelihood of unavailability, duration of unavailability, and impact of unavailability. The literature on IT unavailability, however, mainly focuses on decreasing or estimating the likelihood or duration of IT unavailability: it suggests recovery plans (Azzopardi et al., 2011), Service Level Agreements (Liu et al., 2010), IT replication (Azzopardi et al., 2011), reducing interdependency of systems (Tsai & Sang, 2010; Zambon et al., 2007; Zambon et al., 2011; Azzopardi et al., 2011), focusing on IT users’ culture and training (Westerman & Hunter, 2007), system architecture and support maturity (Hariharan, 2010), Failure Mode Effects Analysis (FMEA) (Ohlef et al., 1978; Chunping et al., 1997), Fault Tree Analysis (FTA), and Reliability Block Diagrams (Beaudet et al., 2006; Chen et al., 2002). However, very few studies focused on understanding the “business impact” of IT unavailability. What occurs after the materialization of an IT availability risk matters more to businesses.

Liu et al. (2010) suggests two approaches to assess the impact of unavailability: impact by lost user productivity and impact by unprocessed business transaction. The former estimates the impact of IT unavailability by basing the calculation on the number of users affected during the unavailability period. The latter, however, bases the calculation on the number of business transactions that could not be processed due to unavailability. According to Liu et al. (2010), the latter provides a better reflection of

---

4 This indicates to the emphasis of strategic management on the importance of a firm obtaining a strategic advantage and improving its position relative to other firms.
business impact as “resources [such as users’ time] are not valuable in and of themselves, but they are
valuable because they allow firms to perform activities ... [rather] business processes are the source of
process approach toward IT availability risk. He mentions that what really matters to an organization is
that the business processes are up and running, therefore, if an IT asset unavailability does not lead to the
discontinuity of the business processes, it would not have important consequences.

However, there is a dearth of impact analysis model based on business processes. To the best of our
knowledge, it is only Time Dependency Model (Zambon et al. 2007) that uses the concept of business
processes to develop a model assessing the impact of IT unavailability. In the model, each business
process node is then linked to several application nodes that represent the applications that support the
individual business process. The application nodes themselves are linked to the database nodes and machine nodes that support them. On the link between the two nodes, the time
that the supported node goes down in the case of supporting nodes outage. However, they did not suggest
a way to estimate the impact or the cost of the business process discontinuity.

A Capability-based Approach to BIA

Nevertheless, this paper claims that what really matters to organizations (e.g. banks) is keeping the level
of their capability (e.g. number of potential money transfers per hour), not necessarily the corresponding
business process. Homann (2006) describes business capability (or simply capability) as what a business
does that creates value for customers (directly or indirectly), and describes business process as how the
business performs or implements the given capability. Thus, a capability (e.g. customer checkout) is the
external, observable, and measurable behavior materialized through one or more business processes (e.g.
self-service checkout and cashier-based checkout).

If a business process (e.g. ATM-based transfer) has a close substitute (e.g. clerk-based transfer, online-
banking transfer, PayPal-based transfer) providing the same capability and it experiences discontinuity,
then there is another business process to produce the same value to the organization, and thus the
capability capacity will not be degraded tremendously. Moreover, in the case of less automated business
processes or processes that can continue to operate using manual intervention, IT unavailability will not
result in strategic consequences such as losing market value (Dynes et al., 2007) as the capability capacity
is almost unaffected. Therefore, IT unavailability influences external or internal customers of an
organization if and only if it degrades the corresponding capability capacity which is defined as the
expected level of performance in terms of units per period of time or some quality measurement
(Homann, 2006). As long as it is unaffected, it’s not a business risk at all. Thus, we hypothesize:

**Hypothesis 1**: IT Unavailability results in strategic risk only if it degrades the corresponding capability
capacity.

**Capability Criticality**

However, not all capability degradations result in strategic consequences. Employee payment, for
example, is not a critical capability to Novartis. If a supermarket loses its Employee promotion capability
or litigation capability for a day or week, it is much less of a strategic risk than losing its checkout
capability. In order for a capability capacity degradation to cause strategic consequences, a capability
must be critical or highly valuable so that its degradation be a strategic risk. The concept of critical
capabilities can be found in the “critical business process identification” step in most Business Impact
Analysis methods such as the ones proposed by Swanson et al. (2002) or Tjoa et al. (2008). But which
capabilities are critical? The literature has identified two kinds of capabilities highly valuable and critical.

**Capability Distinctiveness**

Firstly, if a capability is a source of competitive advantage (or what is dubbed as a distinctive competency
or a distinctive capability) (Barney, 1991; Wade & Hulland, 2004), its degradation results in losing the
source of an organization’s competitive advantage over competitors. Thus, the capability degradation is a
strategic risk to the business. Assume a supermarket which is the only one among its competitors that
offers RFID-based checkout. Thus, customers do not need to wait for each product in the cart to be
When is IT Unavailability a Strategic Risk?

scanned, and by passing a gate, the bill will be instantly printed. This supermarket will not have a competitive edge over its competitors if the RFID-based system is unavailable for a certain period and it is probable that it loses some of its customers. It is worthwhile to note that for a capability to remain distinctive, i.e. rare and valuable, for a long time to provide a sustained competitive advantage (e.g. Walmart's logistic capabilities), it must be non-substitutable, inimitable, and immobile so that it will be difficult for competitors to own it (Barney, 1991; Wade & Hulland, 2004).

**Incapability Distinctiveness**

However, distinctiveness is not the only source of a capability’s criticality. In other words, criticality is not only about obtaining competitive advantage, but also about avoiding competitive disadvantage. That is, the criticality implies that the capability is at par with the norm in the industry expected to be satisfied by any firm (Goldstein et al., 2011; Powel, 2001); or simply called as strategic necessity (Clemons & Row, 1991). If a capability is shared by the company and all its competitors, and the company loses it for any reason, this would make the organization’s rank go down in the set of competitors. Therefore, that capability is a strategic necessity to the organization and its inexistence is a distinctive incapability. For example, if the information system that supports the cashier-based checkout capability of a supermarket is disrupted for a day or two while all other competitors have this system up and running, it would be a Strategic Risk. Thus, a capability is critical if it is either a source of competitive advantage (distinctive capability) or a source of competitive disadvantage (distinctive incapability). Therefore,

**Hypothesis 2:** capability criticality acts as a moderator of the relationship between capability capacity and strategic risk. In other words, if the criticality of a capability is low (high), its capacity degradation results in a low (high) strategic risk.

**IT-Capability Detachability**

As aforementioned, not all capability capacity degradations are strategic risk. Similarly, not all IT Unavailability incidents result in business process discontinuity or significant degradation of capability capacity. A potential disruption of a web-based order placement system of a small company, which relies mainly on phone and fax for running its business, would not be a discontinuity risk (Dynes et al., 2007). This is because the order processing capability is highly detachable from the web-based system. **IT-Capability Detachability (ITCD)** is defined as the extent to which the capability (materialized through all its corresponding business processes) and the underlying IT application are loosely coupled (Tanriverdi et al., 2007). In other words, the more a capability and the underlying IT Application are detachable, the less capability capacity is dependent on the application’s availability. At a high level of ITCD, IT (Application) unavailability has a less chance to result in a significant degradation of capability capacity. If a capability is replicated using several different business processes or the application supports a small, non-critical part of the business process that materializes the capability, then capability capacity would be less affected in the case of the application’s unavailability. Therefore,

**Hypothesis 3:** IT-capability detachability acts as a moderator of the relationship between IT unavailability and capability capacity. In other words, at a high (low) level of ITCD, IT unavailability has a weak (strong) relationship with capability capacity.

The level of ITCD is affected by IT-process alignment and capability replication, which will be explained below.

**IT-Process Alignment**

Dynes et al. (2007) figured out that supply chain business processes that utilize significant automation could be substantially affected by IT disruptions. The reason is that as a business process is more supported by an application (i.e. more activities are digitized), the business process is more dependent on the application to be up and running. Therefore, it becomes more susceptible to IT disruption. The concepts of support and significant automation is equivalent to what Barua et al. (2004) dubbed as process alignment or more precisely as **IT-Process Alignment** which is defined as the degree of fit
between business processes and the underlying information technology to facilitate computer-based communications and information process. 

Strong and Volkoff (2010) looked into the concept of misfit or misalignment of Enterprise Systems and found that there are two types of misfit: deficiencies and impositions. Deficiencies are missing features of the application: the activities, data, interfaces, controls, or roles in the business process that are not supported by the application. Impositions are activities, data, controls, interfaces, or roles that are imposed by the application and are not needed in the business process. Impositions may not affect detachability as much as coverage (the opposite of deficiencies). The more activities, data, interfaces, controls, or roles are covered, the more business process is dependent on the application. Therefore, a high fit between a business process and its underlying application means that it is more susceptible to its unavailability. This means the capability, which is materialized through that business process, is also more susceptible to its unavailability. Therefore, the more IT and process are aligned, it is more difficult to detach capability from the underlying IT. Therefore, 

**Hypothesis 4:** IT-Process alignment has a negative relationship with IT-capability detachability.

To the best of our knowledge, this is among a few studies that discuss potentially undesirable negative consequences of alignment for organization. However, even though IT-process alignment has a negative effect on ITCD and will result in more susceptibility to IT disruptions, organizations try to increase the alignment to enjoy its potential impact on firm performance (Chan & Reich, 2007) and the firm’s ability to realize its goals and objectives (Chan et al., 2006). Nevertheless, organizations need a way to increase their IT-Capability Detachability to lower the risk of capability capacity degradation due to IT Unavailability. This way is called as capability replication in this study.

**Capability Replication**

As mentioned before, a capability can be materialized through different business processes. If there is only one business process that materializes a capability and this business process is highly aligned with the application and thus totally dependent on it, then the capability is also totally dependent on that application which means ITCD is low and thus capability capacity is highly susceptible to IT unavailability. However, if there are other business processes that can materialize the same capability, then ITCD will be higher and capability capacity will be less susceptible to IT unavailability. The state of having two or more business processes materializing the same capability is referred to as capability replication in this study. Capability replication can be achieved by having an outsourcer on call and ready to step in, or a business process that will be run manually (Westerman & Hunter, 2007). Parts of plans such as Business Continuity Plan (BCP), Business Recovery Plan (BRP), Continuity of Operations Plan (COOP), and Disaster Recovery Plan (DRP) (Swanson et al., 2002) deal with capability replication, although they focus on decreasing the likelihood or duration of IT unavailability as well. Having a plan for continuing the business process and recovering it means that the organization has identified business processes to be run without the application even though with a low capacity. Thus, the capability is more separable from the application. Therefore, 

**Hypothesis 5:** Capability replication has a positive relationship with IT-Capability Detachability.

**Control Variables**

We will control for switching cost and customer loyalty. The reason is that if the cost of switching to the competitor for customers is high or the customer is loyal to the firm, then capability capacity degradation will not be a strategic risk even if the capability is a critical one. For example, it might be quite challenging for customers of a bank or students of a university to switch to another competitor even if they frequently experience IT unavailability. However, in the case of Google Drive and Office 360, that offer cloud storage and Software as a Service as a Service, the switching cost for some customers is very low. Thus, if a software firm which uses Google spreadsheet on Google Drive for agile project management purposes (e.g. task assignment, task identification, sharing the tasks with other team members) experiences unavailability, it

---

5 In fact Tallon (2007) and Ray et al. (2004) raised the point that alignment is a process-level concept rather a firm-level concept and should be measured at the process level.
can easily migrate to Office 360 or DropBox to mitigate the risks that endanger its main capability: software producing.

**Methodology**

The main method of the study will be a field survey. However, the model is currently discussed with professors, Ph.D. students, and IT practitioners to check for the validity of the research model and to ensure that the constructs and the relationships were identified correctly. Once completed, a pilot study will be conducted in which 30 organizations will be surveyed to ensure the reliability of the scales and identify questions which are not expressive enough. Then, the main survey will be conducted to empirically test the research model and hypotheses. The sampling frame will be 1000 profit-seeking companies in North America and from various industries that are subscribed to cloud services; government agencies or not-for-profit organizations have less emphasis on strategic management and strategic risks and thus will not be part of the study. The primary respondents will be Enterprise Architects or CIOs who have the required knowledge for answering the questionnaire based on pilot interviews we had conducted. The result will be analyzed using HLM software as we will be asking the respondents to estimate capability capacity and strategic risk under different duration of (3-day, 1-day, and 4-hour) IT unavailability which violates the assumption of OLS-based regression that the observations of dependent variables must be independent (Bryk & Raudenbush, 1992). All the constructs will be measured using multi-item, 7-point Likert scale. The operationalization and definitions of the constructs can be found in Table 1.

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definitions and Items</th>
<th>Supporting Literature</th>
</tr>
</thead>
</table>
| Strategic Risk             | **Definition:** the probability of losing rank position in the set of firms that are producing products or services that are close substitutes for each other  

A 3-day/1-day/4-hour outage of the Cloud Service has a/an ...( Scale A)...... potentiality for: 1) resulting in losing our rank position among the competitors that produce similar product or service. 2) compromising our organization’s long-term position with regards to our competitors. 3) resulting in loss of our market share (customer relationship), financial health, or critical resources or key employees. | (Collin & Ruefli, 1992), (Tanriverdi et al., 2007) |
| Capability Capacity        | **Definition:** the extent to which the expected level of performance of a capability is degraded  (capability is defined as what a business does that creates value for customers (directly or indirectly)  

A 3-day/1-day/4-hour outage of the Cloud Service has a/an ...( Scale A)...... potentiality for: 1) degradation of Capability Capacity, 2) lowering the capacity of the Capability, 3) deteriorating the Capability | (Ulrich & Rosen, 2011; Homann, 2006) |
| Detachability              | **Definition:** the extent to which the capability and the underlying IT application are loosely coupled  

1) The Capability can be kept in a normal status even the cloud service is down. (Scale B) 2) The Capability is ...( Scale A) dependent on the cloud service. 3) The Capability is not reliant on the cloud service. (Scale B) | (Tanriverdi et al., 2007) |
| Capability Replication     | **Definition:** the extent to which the capability has been materialized through two or more business processes  

1) We have one or more other ways to keep the capability in the case of Cloud Service outage. 2) If the cloud service is interrupted, we have other ways to run the business. 3) In the case of cloud service discontinuity, we have a plan to do the job on other ways. (Scale B) | (Westerman & Hunter, 2007) |
| IT Process                 | **Definition:** the degree of fit between a business process and the underlying IT application | (Barua et al., 2004), Strong & |
When is IT Unavailability a Strategic Risk?

<table>
<thead>
<tr>
<th>Alignment</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) All activities, roles, data, and controls to achieve the capability are supported by the cloud service. 2) The cloud service supports all the activities, roles, data, and controls needed for achieving the capability. 3) The cloud service covers all activities, roles, data, and controls we need to achieve the capability. (Scale B)</td>
<td></td>
<td>Volkoff, 2010</td>
</tr>
<tr>
<td>Capability Criticality</td>
<td>Definition: the extent to which a capability is valuable to an organization (a second-order factor acting as a proxy for incapability distinctiveness and capability distinctiveness)</td>
<td>(Barney, 1991; Wade &amp; Hulland, 2004)</td>
</tr>
<tr>
<td>Incapability Distinctiveness</td>
<td>Definition: the extent to which a capability is a strategic necessity i.e. whose non-existence is rare in the set of competitors</td>
<td>(Clemons &amp; Row, 1991; Goldstein et al., 2011; Powel, 2001)</td>
</tr>
<tr>
<td>Capability Distinctiveness</td>
<td>Definition: the extent to which a capability is unique to a company or rare in the set of competitors.</td>
<td>(Barney, 1991; Wade &amp; Hulland, 2004; Tanriverdi et al., 2007)</td>
</tr>
</tbody>
</table>

Table 1 - Definitions and Operationalization of the constructs.

- Scale A: [1]: almost no, very low, low, moderate, high, very high, [7]: extremely high
- Scale B: [1]: Strongly disagree... [4]: Neutral... [7]: Strongly agree.

This study will consider three control variables: industry type, organization size, switching cost and customer loyalty to the organization. Dynes et al. (2007) have found that supply chain processes in oil and gas industry could be significantly impacted by certain cyber disruptions unlike automobile parts manufacturer that could experience minor effects or electrical goods manufacturer that could experience no effects at all. They also have found that small scale organizations are less affected by internet outage. Besides, in case of an IT disruption, loyal customers will wait for their preferred vendor’s systems to recover rather than converting to a rival company (Martinez, 2009).

Contribution for Researchers and Practitioners

This study will contribute to the IS literature and practitioners in several ways. First, there are a few studies on unavailability of operational information systems in IS top journals. Second, almost all studies and frameworks on IT unavailability have focused on evaluating its risk based on the antecedents of IT unavailability or decreasing the probability of IT unavailability risk. To the best of our knowledge, only one study discussed the business issues in terms of cost of business process interruption in the aftermath of an IT unavailability. Third, while almost all frameworks and studies had a Likert scale such as impact, severity, or effect, they have not provided a way to measure this impact or clarify the important variables to think about the problem. This study has identified concepts such as capability capacity, IT-capability detachability, IT-process alignment, capability distinctiveness and incapability distinctiveness in business impact analysis of the outage of an IT application. Fourth, this study emphasizes on the Capability-based approach instead of business process-based or resource-based approach as capability is a more stable concept for business impact analysis and strategic management. In other words, we suggest practitioners and researchers to think about IT unavailability in terms of its effect on the business capabilities of an organization.
Conclusion

With an increasing embeddedness of information systems into the business processes, their failures can lead to significant consequences for organizations (Goldstein et al., 2011). The research question addressed in this study is “when IT unavailability is a strategic risk”. The study will demonstrate that in order for an IT unavailability to be a strategic risk (i.e. resulting in losing rank position in comparison to competitors), the supported capability must be either unique in the set of competitors (distinctive capability) or its inexistence must be unique in the set of competitors (a distinctive incapability). In addition, the IT-capability detachability must be low which means the IT-process alignment must be high and the capability replication must be low. It is worthwhile to note that, as far as we know, this is for the very first time that alignment has argued to have a negative, undesirable role in a study. Currently, we are interviewing practitioners and experts to check the validity of the model. The next step will be conducting a survey of profit-seeking companies that apply Cloud-based services in their business.

References


When is IT Unavailability a Strategic Risk?


