Managing SaaS risk in higher education organisations: a case study


DOI: [10.4018/jebr.2013040102](http://10.4018/jebr.2013040102)

©2013, IGI Global

Reproduced with permission.

Downloaded from DRO: [http://hdl.handle.net/10536/DRO/DU:30077578](http://hdl.handle.net/10536/DRO/DU:30077578)
Managing SaaS Risk in Higher Education Organisations: A Case Study

Indrit Troshani, University of Adelaide Business School, The University of Adelaide, Adelaide, SA, Australia

Giselle Rampersad, School of Computer Science, Engineering and Mathematics, Flinders University, Bedrock Park, SA, Australia

Nilmini Wickramasinghe, Epworth HealthCare & School of Business IT and Logistics & Health Innovations Research, RMIT University, Melbourne, VIC, Australia

ABSTRACT

Software-as-a-Service (SaaS) is a new information and communications technology (ICT) that offers dynamically scalable reconfigurable services to clients on demand via the internet. It is heralded as one of the most significant ICT advances that can facilitate business value creation and innovation. There is paucity of research concerning the perceived risks that can affect SaaS adoption intentions of higher education organisations (HEOs). In attempts to contribute to the existing body of knowledge, this study draws on qualitative evidence to explore perceived SaaS risks at HEOs. It equips HEO managers and policy makers with an integrative risk management framework for SaaS adoption.

Keywords: Adoption, Higher Education, Information and Communication Technology (ICT), Risk, Software-as-a-Service (SaaS)

INTRODUCTION

Software-as-a-service (SaaS) is an arrangement that enables the convenient provisioning of configurable software applications on-demand across numerous host computers that are connected via a network (Mell & Grance, 2010; Svantesson & Clarke, 2010). The software applications are controlled by providers or vendors which consumers can access remotely through thin client interfaces (e.g. web-browsers via the internet) in return for payment of usage fees or even free-of-charge (Gupta & Herath, 2005; Heart, 2010). Popular examples include web-based mail (e.g. GMail and Yahoo Mail) and file sharing applications (e.g. Google Docs and filesanywhere.com).

SaaS has the potential to transform the ICT industry in many ways including changing the way in which software are designed and used resulting in significant business value generation and innovation (Armbrust et al., 2010;
Julisch & Hall, 2010). Specifically, SaaS is expected to result in fundamental organisational impacts in the form of significant efficiency improvements, cost reduction, increased flexibility, and shorter time-to-market, and overall national macroeconomic performance impacts in the form of growth, competition and business creation (Dutta & Mia, 2011; Etro, 2010). Consequently, SaaS is poised for strong growth into the future. For example, Gartner predicts that by 2013 the global SaaS market is forecast to have a 17.7% compound annual growth or reach USD14 billion (Mertz et al., 2009), and that by 2012 at least a third of business software spending will be on SaaS applications (Plummer et al., 2008).

With these growth trends, there are growing calls in the literature for further research concerning SaaS. Whilst existing analyses have been undertaken from the service providers’ perspective, there is need for further research that focuses on the organisational adopters’ perspective (Behrend et al., 2011; Carr, 2005; Clarke, 2010; Haselmann & Vossen, 2011; Jaeger, Lin & Grimes, 2008; Marston et al., 2011; Svantesson & Clarke, 2010). However, there is a wide range of different organisations operating in different industries (e.g. business and management, finance, manufacturing, education, oil and gas, government, healthcare, telecommunications) that are currently contemplating to adopt SaaS with the hope of taking advantage of its espoused value propositions (Ercan, 2010). Given the idiosyncrasies of these prospective adopters (Ercan, 2010), in this paper, we focus on higher education organisations (HEOs) (e.g. universities).

We argue that HEOs are interesting for many reasons. First, as the sector grows, HEOs are increasingly relying on larger numbers of applications (e.g. e-learning and scientific computing) to support teaching and research roles which has resulted in significant cost increases (Liao, 2009; Sheng, Ren, & Wang, 2011; Sun et al., 2007; Xu, Li, & Zhao, 2011; Yang, Zhu, & Zhou, 2011). Second, there is growing evidence that HEOs are facing increasingly tighter public funding constraints (Hyland, Marceau, & Sloan, 2006; Mehta, 2004). Third, Xu et al. (2011) argue that the scale and scope of usage of teaching and research applications at HEOs can change “unceasingly” (p. 114) as needs for these applications change (e.g. teaching period versus non-teaching periods). Also, driven by relatively short and frequent hardware upgrade cycles, teaching and research applications may also need to be updated frequently (Yang, Zhu, & Zhou, 2011). These frequent changes can make traditional software provisioning costly at HEOs, and potentially result in waste of valuable resources, particularly when licensing agreements are inflexible. With these increasing pressures on their cost structures, HEOs are focusing on the delivery of the core competencies of teaching and research whilst looking for innovative cost-effective ways to handle supporting non-core activities, including ICT generally, and software provisioning in particular.

There is agreement in the literature that SaaS can be a cost-effective means for HEOs to achieve these aims by helping them control ever-growing software requirements and costs, thereby, assisting HEOs optimise their utilisation (Behrend et al., 2011; Ercan, 2010; Erkoç & Kert, 2011; Sasikala & Prema, 2010; Sun et al., 2007). For example, SaaS can assist HEOs in replacing software applications traditionally installed on campus computers with applications delivered via the internet, resulting in reduced costs and complexity whilst also eliminating time- and location-related constraints for students and academics and making access to learning and research applications cost-effective, equitable, and encompassing (Behrend et al., 2011; Ercan, 2010; Erkoç & Kert, 2011; Sasikala & Prema, 2010). Whilst SaaS does not necessarily eliminate the need for computer hardware at HEOs, it can reduce costs as older hardware can continue to remain useful for longer whilst software installation and error fixing tasks are carried out centrally by SaaS providers, thereby, potentially extending the useful life of existing ICT resources at HEOs (Behrend et al., 2011; Erenben, 2009). SaaS can also enable HEOs to offer e-learning or distance education courses to
local and international students allowing them greater flexibility to enrol at various courses that rely on learning and research applications whilst also offering commute savings for students who live off-campus (Erkoç & Kert, 2011; Sander, 2008). Additionally, the increasing wide-spread adoption of Web 2.0 applications and services computing constitutes another important reason why SaaS can be useful to HEOs (Erkoç & Kert, 2011).

Major well-known commercial SaaS providers have recognised these trends and opportunities in the higher education sector and are offering SaaS applications to facilitate education activities for both academics and students. For example, Google has designed Google Apps for Education which offers HEOs integrated communication and collaboration tools for educational purposes (Google, 2011).

As SaaS is an emerging phenomenon, there is paucity of research concerning the perceived risks that affect the adoption intentions of HEOs (Heart, 2010; Susarla, Barua & Whinston, 2003). In attempts to address these shortcomings and to add to existing SaaS literature, the goal of this paper is to address the research question:

What SaaS adoption risks are perceived by HEOs?

SaaS is a type of ICT outsourcing (Cullen & Willcocks, 2003; Gorla & Lau, 2010). However, unlike traditional ICT outsourcing whereby providers offer unique and customised services according to the client’s exact terms and specification, SaaS services offered are highly standardised. Providers can offer these services inexpensively in a commoditised “one-size-fits-all” fashion by spreading costs across large consumer bases at a much wider scale, i.e. the internet (Brunette & Mogull, 2009; Datamonitor, 2009; Julisch & Hall, 2010). Thus, whilst SaaS providers can offer low-cost, short time-to-market, on-demand services, the shared underlying SaaS infrastructure across numerous clients “destroys any client’s ability to afford the same level of control known from classic ICT outsourcing” (Julisch & Hall, 2010, p. 300). Nevertheless, like classic outsourcing, with SaaS the contractual terms detailing the agreement between SaaS providers and consumers are specified in Service Level Agreements (SLAs) which can provide clients with some control concerning the extent to which SaaS offerings can be customised to their needs (Cullen & Willcocks, 2003; Julisch & Hall, 2010). The extent to which control is maintained by SaaS clients or ceded to SaaS providers can create uncertainty or risk for clients concerning the various ways in which their core competencies or supporting functions are perceived to be affected due to the move from traditional to SaaS environments.

Identifying and addressing perceived risks are particularly important as they can affect HEO adoption attitudes towards SaaS. Consistent with Carr (2005), we argue that the biggest obstacle to SaaS adoption “will not be technological but attitudinal” (p. 71). Although gaps do exist between subjective public perception of SaaS risks and objective expert assessments, the former cannot be ignored as it can affect adoption intentions in organisations (Chellappa & Pavlou, 2002).

Additionally, recent examples of SaaS failures such as Microsoft’s Danger division’s loss of US’s T-Mobile customers’ data and Google’s unexpected GMail service outage provide evidence that SaaS services can be unreliable in delivering functionality and espoused benefits thereby making concerns about associated risks justifiable (Ashford, 2009; Gaudin, 2011). Thus, in addition to SaaS benefits, HEOs also need to consider the associated risks and corresponding likely effects on their organisations’ ability to deliver core and supporting functions before SaaS adoption decisions can be made (Erdogmus, 2009). Also, as an emerging technology, SaaS will need to prove that it fulfils the numerous ICT standards including security, reliability, stability which have been developed in relation to traditional computing on the basis of decades of experience (Marston et al., 2011).

This study culminates with an integrative risk management framework concerning the organisational adoption of SaaS at HEOs. This framework contributes to the existing body of knowledge by informing prospective adopting
HEOs of technological, organisational, and environment risks which need to be both managed and mitigated before SaaS adoption can succeed and its espoused benefits materialised (Farrell, 2010).

To address our aim, first we discuss the notions of risk, risk management, and the organising framework, namely, the technology-organisation-environment (TOE) framework. Data collection and analysis are explained before the proposed SaaS risk management framework is elaborated. The paper is concluded with a discussion of managerial implications and future research directions.

RISK AND RISK MANAGEMENT

Risk is defined as the possible impact of an event on an organisation’s performance or assets and the corresponding expected and unexpected consequences that occur as a result (Levin & Schneider, 1997; Scott, 2004; Shih, 2010; Stoneburner, Goguen & Feringa, 2002; Wright, 2009). In measurable terms, risk is a statistical measure that encapsulates the consequence of a loss by the chance of its occurrence (Crouhy, Galai, & Mark, 2006). Various disciplines define risk in different ways. For example, medical science adopts the perspective of risk as a probability function (Kobs, 1998). In finance, risk represents the variance of outcome distribution (Levine, 2000; Schirripa & Tecotzky, 2000), whereas casualty insurance views risk as expected loss (Bowers et al., 1986). A managerial perspective of risk in ICT outsourcing associates risk with “danger or hazard” perceptions that can result in negative outcomes (March & Shapira, 1987; Pavlou, 2002; Scott, 2004). In this study, we adopt the managerial perspective of risk. This choice is a useful proposition, particularly, given the emerging nature of SaaS and its pertinence to managers in organisations contemplating to adopt SaaS solutions.

There is widespread agreement in literature that even in established relationships between organisations, risks might exist whether partners have the intention or will to, in fact, act appropriately as specified in ICT outsourcing SLAs (Cullen & Willecocks, 2003; Liang et al., 2005; Shih, 2010; Wright, 2009). These risks can erode relationships and potentially increase costs for both providers and their clients (Rousseau et al., 1998) and may operate in SaaS contexts too (Paquette, Jaeger, & Wilson, 2010). In an emerging area such as SaaS, prospective adopting HEOs may find it challenging to easily and clearly associate risk with well-understood or widely-accepted cost structures (Paquette, Jaeger, & Wilson, 2010).

Closely related to risk is the notion of risk management. In SaaS settings, risk management is the process of developing risk-adjusted strategies that attempt to balance the opportunities that SaaS offers with likely positive and negative consequences of taking advantage of them (Crouhy, Galai, & Mark, 2006; Straub & Welke, 1998). That is, risk management can help deal with the consequences of modification, destruction, theft or unavailability of software services and data that are likely to occur in SaaS settings (Straub & Welke, 1998). Furthermore, in SaaS contexts where sensitive data are held and operations are carried out outside organisational boundaries, risk can increase substantially as client organisations can expose themselves to failure risk or opportunism from their SaaS providers (Liang et al., 2005; Wright, 2009). Examples include misuse, disaster, violation of access privileges and restrictions, intellectual property theft, data loss or damage (Dillon & Lending, 2010; Ghosh, Dhumal, & Chawla, 2012; Moores, Nill, & Rothenberger, 2010; Paquette, Jaeger, & Wilson, 2010). Consequently, clients may want strong guarantees that SaaS providers will not opportunistically share their data with others or that the computing resources that the providers offer will be reliable and impenetrable to illicit hacking activities from both outsiders or even SaaS co-tenants.

As SaaS is a type of outsourcing, if one is to understand risks associated with it, “it is essential to identify the array of potential undesirable outcomes that could occur with respect to the outsourcing [or SaaS] arrangement” (Aubert, Patry, & Rivard, 2005, p. 12).
Therefore, understanding and undertaking risk management relevant to SaaS settings are of paramount importance for HEOs that intend to take advantage of SaaS capabilities. Whilst risk management can be complex and ensuing outcomes or consequences not necessarily precise, identifying SaaS risks is the first step that can allow these risks to be managed and mitigated (Paquette, Jaeger, & Wilson, 2010).

**ORGANISING FRAMEWORK**

We consider SaaS as an innovation which various organisations are considering to adopt. One of the most established approaches in studying innovation adoption entails identifying contingency factors that can affect adoption decisions in organisations (Fichman, 2004). Also known as “innovation configuration” (Fichman, 2004, p. 320) these factors can jointly explain adoption outcomes in organisations, and are commonly classified into three broad contextual categories, namely, technology, organisation, and environment (TOE) (Chong et al., 2010; DePietro, Wiarda, & Fleischer, 1990; Shropshire, Warkentin, & Johnston, 2011; Tornatzky & Klein, 1982; Troshani, Jerram, & Rao Hill, 2011). The TOE framework can be useful for the systematic and structured analysis of innovation adoption in organisations, in that, it helps distinguish between the intrinsic characteristics of innovations, organisational capabilities and motivations, and broader environmental dimensions that impact on organisational adopters (Dedrick & West, 2004).

First, the technology context focuses on the manner in which technology characteristics can influence adoption (Chong & Ooi, 2008; DePietro, Wiarda, & Fleischer, 1990; Pedroso, Zwicker, & de Souza, 2009; Tan et al., 2009; Yang, Lee, & Lee, 2007). Second, the organisational context describes the nature of organisational characteristics, including structures, processes, and resources, that may facilitate or inhibit adoption (DePietro, Wiarda, & Fleischer, 1990). Third, the environment context represents the arena where organisations conduct their business, and includes industry characteristics, government regulation, and supporting infrastructure (Chong & Ooi, 2008; DePietro, Wiarda, & Fleischer, 1990; Oliveira & Martins, 2010). Taken together, these factors can present opportunities to encourage organisations to, or inhibit them from adopting innovations such as SaaS.

We argue that risks can affect SaaS adoption because these are factors that can impact on an organisation’s assets and performance outcomes when their corresponding expected and unexpected consequences eventuate (Levin & Schneider, 1997; Stoneburner, Goguen, & Feringa, 2002). Therefore, using the TOE framework as a basis for identifying SaaS risks at HEOs, and subsequently, developing a risk management framework is not unreasonable (Gupta & Herath, 2005; Heart, 2010). Additionally, a review of extant technology assessment literature suggests that it is consistent with the TOE framework (Hensiksen, 1997; Tran, 2007; Van Den Ende et al., 1998).

**DATA COLLECTION**

This research is exploratory and employs qualitative evidence. Given that SaaS adoption is still at an emerging stage, a better understanding of the potential risks that are associated with it can be obtained by examining qualitative interpretations of the relevant stakeholders as they are affected by the potential adoption of SaaS (Van de Ven & Rogers, 1988; Wolfe, 1994). We used a focus group to collect qualitative data (Krueger & Casey, 2000; Malhotra et al., 1996). The aim of focus groups is to elicit participants’ attitudes, perceptions and feelings about new topics. This was consistent with our aim of eliciting risks in SaaS settings. Focus groups are suitable for exploratory research where the field of study is relatively new.

The focus group technique was used to provide a quick and cost-effective way for collecting rich data in a relatively new domain such as SaaS. It enables focus group participants to openly express their views whilst interacting with others in the group. It also provides opportunities for clarification and expansion on
arguments to be made. Consequently, we found
the focus group technique to be an invaluable
tool not only for investigating the participants’
thoughts but also for understanding how ex-
pressed views evolve as participants justify them
to others in the group. Additionally, we found
that new ideas were being generated as partici-
pants could build on arguments based on each
others’ responses. This enabled the generation
of insights that might have not otherwise been
identified using alternative techniques such as
in-depth interviews and surveys.

The aim of the focus group was to explore
the perceived risks concerning SaaS adoption
at an Australian HEO. The focus group was
comprised of fifteen representatives of various
functional areas at the HEO, including admin-
istration, human resources, accounting and
finance, ICT, and academia including sciences,
healthcare, education, architecture, law, and arts.
The representatives were individuals who were
considered knowledgeable on the relevant topics
in their respective areas. The focus group met
in four separate sessions which were organised
by the same moderator. Each session lasted
approximately 90 minutes. In the first session,
the moderator prompted participants with some
general topics and issues recognised as relevant
in extant literature. The objective of each session
was to refine and elaborate the topics and issues
identified in previous sessions and even identify
new ones as applied to the various functional
areas at the HEO. This stepwise refinement
was repeated until all issues were exhausted
and agreement concerning respective clarifica-
tions was reached or until disagreements were
explained or resolved.

The contents of the collected data were
analysed thematically. Codes were developed
which provided the basis for analysis and
helped identify and analyse emerging pat-
terns of themes (Carson et al., 2001; Miles &
Huberman, 1994). Data belonging to themes
were incrementally assembled before being
triangulated against extant literature. Although
the focus group participants represent various
functional areas within the same HEO, we found
that their potential SaaS adoption objectives
were consistently suggesting that integrating
their views is not unreasonable.

Construct validity has been adequately ad-
dressed. First, multiple sources of information
were used (Yin, 2003). Whilst the information
collected via the focus group constitutes the pri-
mary source of information, many focus groups
members also provided supporting secondary
data comprising white papers which were used
for triangulating findings. Second, the focus
group members belong to different functional
areas within the same HEO, and therefore, pro-
vided different perspectives which constitutes
further triangulation of qualitative information
by preventing biased opinions (Carson et al.,
2001; Miles & Huberman, 1994). Third, three
investigators analysed the data thereby reducing
potential bias (Yin, 2003). Finally, the chain of
evidence tracing conclusions to focus group
data was also maintained. According to Yin
(2003), these enhance construct validity and
reliability of this research, thereby boosting
its overall quality.

TECHNOLOGY, ORGANISATION, AND
ENVIRONMENT RISKS

In this section we classify the identified risks
into three broad categories, namely, technology,
organisation, and environment as guided by the
organising framework discussed previously.

The specific risks that have been identified in
relation to SaaS at the HEO have been sum-
marised in Figure 1. These risks are discussed
in further detail in the sections that follow.

Technology Risks

- **Malicious Activity**: SaaS can be suscep-
tible to malicious activity by i) SaaS pro-
vider insiders, and ii) outsiders or hackers
including SaaS co-tenants. The first type
of malicious activity concerns situations
whereby individuals can abuse their high
privilege roles in their capacity as SaaS
provider employees. For example, roles
such as system administrators, security
providers that analyse intrusion detection, auditors, etc. constitute high privilege roles within SaaS providers. The second type of malicious activity concerns hacking by outsiders or even SaaS co-tenants that attempt threats, such as, malicious probes, scans, and network mapping. Malicious activities can potentially lead to loss of data integrity, confidentiality, and availability, potentially leading to economic loss, diminished customer trust, and damaged reputation of HEOs.

- **Data Transit Risk:** Due to their distributed nature, at any given time, in SaaS settings larger amounts of data are likely to be in transit than in traditional computing environments. Data transfers will occur between the SaaS provider infrastructure and remote web clients for synchronisation, storage or processing purposes. This, however, may increase exposure to eavesdropping threats including sniffing, email wiretaps, and spoofing. Whilst data transit risk can have serious consequences for HEOs it can be mitigated using available encryption technologies.

- **Inadequate Technical Support:** Evidence suggests that current SaaS providers operate self-service type support and provide administrative functions enabling HEOs to apply self-fixes. However, this level of support may be perceived to be inadequate, particularly because traditional computing infrastructures at HEOs operate helpdesk type support which is generally perceived to be efficient and effective by both academics and students. Inadequate helpdesk support is perceived to adversely impact the productivity of HEOs. This risk could be mitigated by either providing helpdesk type support that is effective, efficient and that operates in the HEO’s time zone.

- **Inadequate Data Storage and Retrieval:** In order to ensure that business continuity is at least maintained (if not improved), HEOs need to be able to store and retrieve...
their data both in a timely and cost-effective manner and in accordance with their requirements. Consequently, SaaS providers need to ensure that their underlying infrastructure offers adequate bandwidth and capacity to meet existing business needs of their clients with flexibility as HEOs grow in response to changing environments and teaching and research requirements. HEOs can mitigate risks of this nature by including relevant clauses in SLAs with SaaS providers concerning both critical levels of functional specifications and reasonable fees that may be charged by providers.

• **Limited Expertise:** Whilst SaaS providers can offer various computing capabilities, HEOs also require adequately skilled human resources that can manage the interface between themselves and their SaaS providers. There was agreement in the focus group that there is currently limited expertise available including knowledge, experience, and skills, in managing SaaS provider relationships within HEOs. Whilst this risk can adversely affect the experience of HEOs with SaaS, it can be mitigated by way of training and recruitment.

**Organisation Risks**

• **Lock-in Risk:** This risk may emerge to become a serious threat on HEO operations if or when service or delivery performance offered by SaaS providers deteriorates overtime. Additionally, potentially disastrous failure can result in situations when SaaS providers face bankruptcy, terminate their services or are acquired by other SaaS providers. In these scenarios HEOs may have to migrate from one SaaS provider to another which may result in disruption of core teaching and research functions. This risk may be mitigated by ensuring that optimal performance indicators are prescribed in SLAs and that SaaS providers offer adequate tools, procedures, and standards that can guarantee seamless data and capability portability.

• **Intellectual Property (IP) Loss Risk:** This risk concerns perceptions that IP may be lost as commercial and confidential type of information concerning research is transferred to and stored in SaaS environments. Exposure of such information may increase legal liability of HEOs. Focus group informants were consistent in pointing out that IP loss risk can be mitigated in various ways. For example, HEOs can specify clauses in contractual agreements that using SaaS capabilities does not cede IP rights to SaaS providers. Additionally, HEOs can select SaaS providers that operate in national jurisdictions which protect IP in ways that are similar to what is afforded by Australian legislation.

• **Security and Privacy Breaches Risk:** This risk is related to perceptions amongst HEO users that security with existing traditional in-house architectures is higher than in SaaS architectures. However, there was agreement amongst informants that these perceptions are incorrect and not justified, and that security in SaaS architectures can, in fact, be higher than in traditional in-house ICT environments. Additionally, privacy breach risk is considered to be important particularly in cases where confidentiality breaches are not reported to HEOs by their SaaS providers. Both security and privacy breaches can result in serious economic loss due to potential disruptions of core teaching and research operations, litigation due to loss of commercially-sensitive or personal data (e.g. innovations or healthcare data). Taken together, these can become major and serious pitfalls that offset SaaS benefits and that are likely to undermine the sustainability of HEO confidence on SaaS settings. Security and privacy breaches risk can be mitigated by providing awareness sessions to reassure users concerning security levels that SaaS environments can offer.

• **Loss of Control Risk:** Migration to SaaS environments entails ceding control of computing capabilities to SaaS providers. There are negative perceptions associated
with this amongst HEOs as loss of control is seen as dependency on SaaS providers which can adversely affect their control to service delivery and quality including contingency procedures, such as, disaster recovery, backup and restore functions. For example, SaaS providers may outsource specialised functions which can extend HEO dependency to third parties thereby potentially complicating both coordination chains and recourse to remedies in cases of non-compliance with SLA specifications. Additionally, HEOs may have less bargaining power with larger and reputable SaaS providers whilst contract enforcement can be costly and difficult particularly if SaaS providers are outside Australia which is more likely than not. This was unanimously considered to be a high risk, but which could be mitigated by way of contract negotiation and specification of legally binding terms and conditions in SLAs.

Environment Risks

- Cross-Jurisdictional and Data Sovereignty Risks: It is expected that SaaS providers operate their capability offerings outside Australia. SaaS services used by HEOs will, as a consequence, be subject to the host countries’ legislation and, therefore, exposed to cross-jurisdictional risk (Pearson & Charlesworth, 2009). This risk is often referred to as data sovereignty risk (Gambotto-Burke, 2010). Data sovereignty was considered to be highly risky, particularly when host countries’ legislation changes frequently, is unpredictable, is not enforced consistently, is inconsistent with or does not adhere by international agreements. Corollary issues include scenarios whereby SaaS providers are subpoenaed by law enforcement organisations whereby SaaS hardware can be confiscated for e-discovery. Common examples that were cited by informants and substantiated in the literature are the USA Patriot Act and the Homeland Security Act which significantly reduce restrictions on US law enforcement agencies’ ability to access data held in servers within the United States (Gambotto-Burke, 2010). These situations can potentially result in confidentiality and data security breaches, data leakage, and economic loss for HEOs which constitute some of the primary concerns why many organisations have been reluctant to move to SaaS settings. A related concern to cross-jurisdictional and data sovereignty is the issue of where data could end up. For example, an Australian HEO uses a SaaS service which is located in Singapore but which is backed up in Hong Kong or China. In situations of this nature, SaaS providers need to be able to reassure HEOs that data privacy obligations are fulfilled and maintained when data is held in multiple possibly different jurisdictions. Although this was considered to be a high risk with potentially serious consequences, it can be mitigated by way of contract negotiation. That is, including clauses requiring full disclosure and negotiation concerning data storage and back up locations.

- Impact of Local Legislation Risk: Local legislation and regulation constitute another factor that can inhibit or drive adoption of SaaS capabilities. For example, when patient health data is moved to SaaS settings various types of regulations can come into play. Although focus group members were not aware of issues arising due to local (Australian) legislation restrictions at the time of the data collection, they cited international examples to substantiate this point. For instance, in the US, regulations such as the Sarbanes-Oxley Act (SOX) and the Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) restrict where financial reporting and health data can be stored, respectively, which can also restrict the manner in which SaaS solutions are adopted by HEOs.

- Media Exposure and Scrutiny: Another risk raised in the focus group. As HEOs rely on prominent SaaS providers they may...
suffer media scrutiny when these providers experience failures. Failures of traditional computing capabilities were not considered to be as exposed to media scrutiny as those in SaaS settings (Ashford, 2009).

**DISCUSSION**

We have identified three different risk management perspectives and integrated them into a single framework which can improve current understanding of emerging and complex phenomena concerning SaaS adoption within HEOs whilst also adding to existing embryonic SaaS literature. We have discussed some of the possible impacts of these risks and some possible ways in which HEOs can mitigate them. Whilst our analysis of SaaS risks is not meant to be exhaustive, rather a starting point for further investigations, it is consistent with and responds to calls in extant research for considering SaaS risks from the user’s perspective (Carr, 2005; Clarke, 2010; Jaeger, Lin, & Grimes, 2008; Marston et al., 2011; Svantesson & Clarke, 2010). We have adopted an integrative view of these risks by adapting the well-known TOE framework for a risk management perspective at HEOs in SaaS settings. Adopting an integrative view can provide academics and practitioners alike with a useful holistic tool for explaining the complex phenomenon of SaaS risk management. This is important as the future pace of SaaS adoption at HEOs is dependent upon how quickly the identified risks can be mitigated (Qamar, Lal, & Singh, 2010). Additionally, if these risks are considered as SaaS is still evolving they may be mitigated before consequences of ignoring them become too significant and adversely affect the quality of SaaS solutions in the long term (Jaeger, Lin, & Grimes, 2008).

Although the economic and social motivation for SaaS is high, prospective HEO adopters need to be cautious when making adoption decisions. There is evidence to suggest that there are many organisations that are adopting SaaS solutions while being oblivious of the possible risks and associated implications of putting sensitive data and critical applications on SaaS settings (Popović & Hocenski, 2010). Thus, awareness of SaaS risks is important to both HEO adopters and SaaS providers. On the one hand, HEOs need to be aware of the possible ways in which teaching and research operations can be affected as they are delivered through SaaS solutions. On the other hand, SaaS providers need to know of the vulnerabilities of the solutions they offer in order to provide remedies to alleviate HEO concerns, meet SLA obligations, and prove compliance to auditors (Popović & Hocenski, 2010). Furthermore, if HEOs are not confident that SaaS providers can offer security, privacy, and reliability assurances then many will probably opt not to adopt available solutions. It is, thus, vital for SaaS providers to identify and mitigate SaaS risks to both address HEO concerns and to fulfil their SaaS profitability objectives (Jaeger, Lin, & Grimes, 2008).

Early evidence shows that efforts are underway to address some identified risks in various forms. For example, in attempts to address cross-jurisdictional and data sovereignty risks some ICT companies (non-HEOs) in Australia are creating their own private SaaS services. Whilst these strategies can address security and confidentiality concerns they can also create capacity and cost implications which can offset cost-saving benefits associated with SaaS adoption (Gambotto-Burke, 2010). In another example, in attempts to address cross-jurisdictional and data sovereignty concerns and satisfy data regulation requirements of specific jurisdictions major SaaS providers are now offering services to locations specifically covered by those jurisdictions. For example, Amazon Web Services (AWS) recently announced that it is going to locate its Amazon SimpleDB storage service physically to the European Union specifically to address the Binding Corporate Rules (BCRs) which constitute data regulation requirements allowing international organisations to transfer personal data across borders without violating the EU Data Protection Law (Amazon, 2011). Similarly, data protection mechanisms are implemented in other regions...
such as the Cross Border Privacy Rules in the Asia-Pacific Economic Cooperation (APEC) countries which need to be taken into account by SaaS providers in order to address cross-jurisdictional and data sovereignty risks (AustralianGovernment, 2008). Thus, given the cross-jurisdictional nature of SaaS solutions it is possible that identical data collected in different jurisdictions or contexts by different SaaS providers may be subject to divergent legislative and regulatory regimes which suggests that if SaaS providers are to establish full disclosure and transparency they need to provide context-specific assurances to HEOs (Pearson & Charlesworth, 2009).

IMPLICATIONS

Given the rich nature of collected data, implications can be derived which can provide insights to both managers in relation to SaaS adoption risks at HEOs and those within SaaS providers. First, the existence of risks may slow down SaaS adoption in HEOs. Thus, knowledge and appreciation of these risks can offer HEO managers that are contemplating to adopt SaaS capabilities, improved insights into balancing specific decisions concerning potential risks. It can also help policy-makers and government regulators design concrete proactive monitoring and intervention policies that offer sensible standards and regulation that mitigate these risks and enhance adoption without stifling innovation, including international agreements favouring data flows across national borders guaranteeing data security and privacy, fiscal incentives to stimulate adoption, and expansion of broadband infrastructure and capacity as necessary prerequisites (Etro, 2010; Marston et al., 2011). Additionally, knowledge and awareness of SaaS risks can also help regulators formulate legislation that demands greater precision in SLAs between providers and HEOs (Jaeger, Lin, & Grimes, 2008). Also SaaS providers can use the findings as a basis to improve their offerings (Mell & Grance, 2010; Svantesson & Clarke, 2010).

Second, given its integrative nature, the proposed framework may better position HEOs with SaaS ambitions to carry out indepth analyses of the SaaS capabilities that they might be considering to adopt. In doing so, HEOs can analyse their strengths, weaknesses, threats, and opportunities and the manner in which the adopted capabilities can help enhance or minimise these in enhancing their positions.

Third, HEO managers need to become cognisant of the relevant legislation in their host country where SaaS capabilities will be based which may be different to the rules under which they may used to operate. A deep understanding of host countries’ institutional contexts may be critical for risk minimisation for SaaS adopters (Mell & Grance, 2010; Svantesson & Clarke, 2010). It may also help SaaS providers become selective and take appropriate steps to assess countries or jurisdictions before making hosting decisions for their offerings.

Finally, given the anticipated sharp rise in the organisational adoption of SaaS and its pervasiveness, inclusion of SaaS risk education in education and training curricula at HEOs may be important in order to produce information system professionals that are mindful to SaaS risks being attuned to addressing them adequately (Jaeger, Lin, & Grimes, 2008).

CONCLUSION AND FUTURE RESEARCH

SaaS is a unique technology that has the potential to become ubiquitous and offer significant economic and social advantages to prospective HEO adopters. These advantages and increasing economic pressures are likely to drive HEO procurement of ICT services into SaaS settings. We have identified a host of technology, organisational, and environment risks of which HEOs need to be mindful as these can present challenges and adversely affect SaaS adoption (Qamar, Lal, & Singh, 2010; Wyld, 2010).

Whilst using a single focus group to isolate potential risks associated with SaaS at HEOs, we appreciate that a limitation is that the risks
examined are based on only one focus group comprised of fifteen members which are part of the same organisation, thereby providing potentially limited insights for generalising to the wider population of prospective HEO adopters across Australia and more broadly worldwide.

Additionally, a limitation of the focus group is possibility of “group think”, that is, the possibility that respondents expressed opinions that are in line with those of the group, though different or opposite to their own. The issue with specific individuals attempt to dominate the focus group discussion, thereby creating an inaccurate view of the group opinions is another concern. Whilst these limitations were addressed in this study by using a skilled moderator, we urge future research to consider our findings in the light of these limitations (Krueger & Casey, 2000; Malhotra et al., 1996).

However, given the exploratory nature of this study, generalisation was not an objective. We accept that the extent to which our findings are useful in practice can be deemed to be tentative without further research investigating SaaS adoption risks from other perspectives in both Australian and non-Australian HEOs.

Additionally, many of the risks that we have identified can be hard to quantify. To avoid common damaging tendencies of practitioners to treat identified risks equally, future research should attempt to examine and measure the true nature and impact of these risks across HEOs as well as the likelihood of their occurrence (Wyld, 2010). Finally, there is agreement in the literature that, as with any new technology, successful adoption of SaaS may entail changes including structural and process changes within HEOs. Thus, further research is needed to address i) the manner in which traditional ICT department roles will change as HEOs’ ICT requirements shift to SaaS settings, and ii) the political implications that arise as HEOs’ ICT departments’ control over ICT resources diminishes.

REFERENCES


Gambotto-Burke, A. (2010). Get IT out there: Cloud computing circumvents the need for owning hardware and software but is it worth the risk. *InTheBlack, 80*(6), 49–53.


