Up in the Cloud: Managers, Employees, and Security Training for Cloud Computing to Avert Cyber Threats

Lisa Kahle-Piasecki
Tiffin University

Matthew E. Ritzman
University of Toledo

Doug Ellingson
Tiffin University

Using cloud computing for applications and the storing of data has become common in today's workplace. Employees frequently utilize cloud computing for its benefits without fully understanding the risks and potential security issues involved. Managers have a responsibility to make sure employees are aware of the possibilities of technology vulnerability. This paper will examine the common uses of cloud computing in today's organization and the steps managers can take to ensure employees are properly trained.

INTRODUCTION

Employees in many large and small organizations routinely access applications from "the cloud" or store data "in the cloud" without understanding the security risks behind the use of the applications and storage of sensitive company information. Managers have a responsibility to ensure organizational data is secure and that employees are trained and knowledgeable on cloud computing. Some of the most common uses of cloud computing in organizations are accessing software applications and/or storing data. In accessing application software, users install and operate software in a business model known as software as a service (SAAS). In this model, a cloud provider installs and operates application software in the cloud. Cloud users access the software, but they do not manage the cloud infrastructure and platform the application runs on. The user is renting or borrowing online software instead of actually purchasing and installing it on their own computer. This is a benefit for customers looking to avoid a large initial investment, which is especially appealing for small companies and startups (Wei et al., 2013).

Entire businesses and thousands of employees run their computer tools as online rented products (Gill, 2015) and this use is projected to continue to grow. Global Digital Infrastructure (2015, November), conducted a survey of 1,212 respondents. Results found that cloud spending continues to outpace overall information technology (IT) spending in their organization. Further, 46% of organizations using the cloud, expect to increase their spending over the next 90 days. In another survey by Global Digital Infrastructure (2015, May) 70% of respondents reported using SaaS when asked which type of cloud the

organization is using. These same respondents reported their organization spends more than 30% of their IT budget on cloud computing. The company Cisco, reported that global cloud traffic will account for more than two-thirds of total data center traffic by 2017 and this will increase at a compound annual growth rate of 35% from 2012 to 2017 (Bildosola, Rio-Belver, Cilleruelo, & Garenchana, 2015).

While there is some debate over who is actually responsible for establishing cloud computing, it is rooted in the 1960s with the development of a global network for computing resources (Mohamed, 2009). Cloud computing is defined as a model for"enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST, 2011, p. 2). The word "cloud" is used to describe, "things happening elsewhere" (Weinberger, 2015). The diagrams that computer scientists and engineers put together to show how devices interacted and exchanged information resembled a cloud, hence the name was accepted.

Cloud computing is seen by industry experts as an innovation that is revolutionizing IT because it is substantially changing the way IT is now consumed as a service much like common utilities such as water, electricity, and telephone services (Evangelista & Nato, 2015). This is a disruptive change that is radically altering the industry's rules for both consumers and providers of cloud computing services and it has a great impact on the global economy (de Borja, 2012). As a result, IT departments may be organizationally restructured to reflect that cloud computing can be an alternative to in-house IT services or as an addition (Choudhary & Vithayathil, 2013). Some IT departments have chosen to source services from several different vendors, such as using one provider for e-mail, another for basic storage and backup services. Working with different vendors allows organizations to get the best price, and structure their IT department accordingly.

A number of businesses have been significant in introducing cloud based software applications and cloud-based services. One pioneering business is Google. Google Docs is known as a SaaS office suite, which is a cloud computing document sharing service. The introduction of Google Docs, allowed users to access the software which is used for creating documents, spreadsheets and presentations, through their browser and automatically save the files to Google's servers rather than purchasing the software. Other popular cloud computing applications (or apps) offered by Google include Gmail, Google Drive, Google Hangouts, and Google Calendar. More than five million organizations worldwide use these applications including 60% of Fortune 500 companies (Nieva, 2014).

CLOUD COMPUTING IN THE EUROPEAN UNION

Despite the predictions of impressive growth, the cloud computing industry in Europe will lag behind the United States mainly as a result of European privacy rules, multi-country business processes and a deep Euro crisis (Gartner, 2012). Cloud computing is associated with a myriad of complex privacy issues; these issues are not new, or even exclusively associated with cloud computing as globally accessible websites have faced similar issues (Svantesson & Clarke, 2010). When cloud computing users utilize a cloud computing service across an international border, they must abide by applicable privacy laws. The most prominent of these laws is European Directive 95/46 (Svantesson & Clarke, 2010). The Directive intended to eliminate obstacles to flows of personal data to promote economic activities, and offer protection of individual rights (Mantelero, 2012). Article 25 of the directive reads:

> "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

Svantesson and Clarke (2010) explained this type of provision places significant limitations on companies who may consider using trans-border cloud computing. Article 25 of the Directive allows

trans-border data exchange from Europe to other countries only in situations when the country in question provides an adequate level of privacy protection (Mantelero, 2012). The directive causes countries that desire to pursue commercial relationships with the European Union to implement similar data protection laws as they are not able to work with European partners without similar standards in place (Mantelero, 2012). Provisions similar to those cited in Article 25 of European Directive 95/46 are important to privacy protection; as such cloud-computing providers will have to develop products that are geographically limited (Svantesson & Clarke, 2010).

BENEFITS OF CLOUD COMPUTING

Cloud computing offers several benefits to organizations where it is utilized. Organizations can source many IT services from the cloud on-demand and with pay-as-you-go pricing (Choudhary & Vithayathil, 2013). This results in the organization eliminating some of their fixed IT costs and can lead to a higher quality of IT services. The organizations do not have to maintain the software since the providers maintain updates and the cost is decreased as each organization does not have to employ highly qualified technicians. Other important benefits of cloud computing include broad network access, and resource pooling.

E-learning

From a talent development perspective, employees can utilize cloud computing for learning and knowledge management. E-learning systems utilized in organizations can use the cloud for SaaS. There are e-learning applications that are free or low cost. A large benefit of this is that employees can learn independently, on their own time, in their own space, and they do not have to deal with computer technicalities (Mitakos, Almaliotis, Diakakis, & Demerouti, 2014). The increased prevalence of mobile broadband internet and upgraded capabilities of mobile devices like tablets and smart phones has provided companies, learners, and educators alike a tool to facilitate learning (Andronie & Andronie, 2014). This also saves cost for organizations as it eliminates the need to hire trainers to deliver instruction.

Employee Training

Introducing a new technology can be met with employee resistance. Training can be an effective tool for managers to prepare employees for the change by providing knowledge and communication before cloud implementation (Bildosola et al., 2015). Organizationally, managers will need to overcome the ineffectiveness of familiar practices by employees when dealing with a new technology (Bildosola et al., 2015). Training provides an avenue to introduce and further develop knowledge and facilitate learning among employees. Evaluation of training interventions should include assessment of the learner's knowledge to ensure understanding of the topic (Pershing, 2006; Novak, 1998).

As the world is rapidly becoming smaller, it is important that management and all employees understand how to keep their intellectual property and company information protected throughout the use of cloud computing. However, "a recent survey from the International Association of Administrative Professionals shows that while the number of office professionals using mobile devices and cloud apps has increased, the level of training has not kept up" (Skidmore, 2013, para.1). On the other hand, this statistic could be easily changed by using some of the many inexpensive or even free resources out there. Organizations such as Lynda and Cloud Academy have begun to see the opportunity to provide training resources to professionals. Solutions such as these provide on-demand training that employees can access through many different mediums. Also, many universities are beginning to offer consultations to organizations in order to train employees on the dangers of cloud computing and solutions to make it safe. Using a consultant can be a low-cost and effective way to train employees and entire organizations on the dangers of cloud computing and how to protect the valuable information that can be stored in the cloud.

Even with these benefits, there is "a lack of knowledge concerning what cloud computing is, as well as its most significant benefits" (Bildosola et al., 2015, p. 2). This lack of knowledge regarding the

benefits is seen as "the greatest obstacle to entry into the cloud" (Bildosola et al., 2015, p. 2). A large number of companies, especially small and medium-sized companies are not aware of cloud technology or potential benefits to organizations (Bildosola et al., 2015).

RISKS OF CLOUD COMPUTING

Although the benefits organizations receive by using cloud computing are significant, there are risks involved, mainly related to information security and potential disruption of service. A study of Brazilian public sector organizations considering whether to start a cloud project (Evangelista & Neto, 2015), found that none of the organizations in the study could adopt SaaS services safely. This was due to poor performance on key management processes researchers determined were necessary for successful implementation. These processes include aspects related to information security and monitoring the IT environment.

Svantesson and Clarke (2010) outlined the risks associated with cloud computing. The authors described risks related to: the security of the data provided; how data provided to a cloud computing operator will be used by the operator; how data will be disclosed by the cloud computing operator, and potentially used by third parties; disruptions of the cloud computing service; entering into a contract for services that may not meet the future needs of the organization; and violating privacy laws by using cloud products.

Many large companies have encountered various security hacks as well as threats of security hacks, including International Business Machines Corporation (IBM) and Target. "IBM says its researchers regularly receive taunts from Russian hackers who leave them mocking messages in software aimed at stealing from the 300 banks IBM serves" (Hardy, 2014, para. 4). This threat is a constant reminder that there is always someone out there who is ready to do whatever it takes to get their hands on IBM's information. Should IBM be hacked, it would put countless people at risk as their private information could go along with it. No company knows this as well as Target. When Target was hacked, the hackers stole millions of debit and credit card numbers that the card holders entrusted Target to protect. JPMorgan Chase has had to replace "2 million credit and debit cards due to the hack" (Ellis, 2014. Para. 1). This demonstrates the risks involved should a company the size of Target and JPMorgan Chase be hacked.

While many large companies constantly have to be on the lookout for breaches in security, individuals also need to protect their own information. Many people have come to believe that Apple products and the Apple cloud are unhackable. However, as Wired technology journalist Matt Honan will be the first to say, this has recently been proven false (Kelly, 2012). "In a chain of events that Honan would unravel in the following days, hackers took advantage of security holes at Amazon and Apple to gain access to his iCloud account" (Kelly, 2012, para. 1). Millions of individuals trust the cloud that Apple and many other companies offer to protect their information for them. However, people need to be aware of the risks involved and work to actively protect their own personal information.

While it may seem like a simple fix, it has been proven by some of the most intelligent minds in the United States that it can be very difficult to prevent cloud computing security breaches. The United States government constantly faces cyber threats from other countries and terrorist groups. Recently, the government systems were hacked into and it is believed that "the attackers who breached State are also believed to be behind hacks on the White House's email system, and against several other federal agencies" (Perez, 2015, para. 2). This is another instance that demonstrates why everyone needs to be aware of and on the lookout for any possible threat to security. Hackers are constantly developing new ways to get into personal information, so individuals, companies of all size, and even the government need to be aware of these new tactics so that breeches in security such as these can be prevented in the future.

IMPLICATIONS

With the projected increase in the usage of cloud computing, organizations are becoming vulnerable to the risks of using the cloud without first providing employees with training and knowledge of both the benefits and purposes of the cloud in the workplace. As more small businesses and organizations begin to use the cloud, they are often at a greater risk than larger businesses because they frequently lack a formal IT department and training and development function. Organizations, both large and small, however need to address what is often a security risk by first providing training for their employees and establishing performance standards for managers to implement with their staff. Secondly, organizations need to be aware of the security measures in place with the cloud providers they are using for services and software.

Universities are adopters and users of cloud computing. They can play a role within their community by designing cloud computing workshops and security training for small businesses and organizations. They can also provide research and awareness of continuing trends and uses of the cloud for the businesses and organizations in their community.

REFERENCES

Andronie, M., & Andronie, M. (2014) Information and communication technologies (ICT) used for education and training. *Contemporary Readings in Law and Social Justice, 6*(1), 378–386.

Bildosola, I., Rio-Belver, R., Cilleruelo, E., & Garechana, G. (2015). Design and implementation of a cloud computing adoption decision tool: Generating a cloud road. *PLoS ONE, 10*(7): e0134563. doi:10.1371/journal.pone.0134563

Choudhary, V., & Vithayathil, J. (2013). The impact of cloud computing: Should the IT department be organized as a cost center or a profit center*? Journal of Management Information Systems, 30*(2), 67-100.

De Borja, F. (2012, October 12). How cloud computing is affecting everyone. Retrieved from http://cloudtimes.org/2012/10/12/how-cloud-affecting-everyone/

Ellis, B. (2014, January 16). Millions getting new debit, credit cards after Target hack. Retrieved from http://money.cnn.com/2014/01/15/pf/new-cards-hack/index.html

Evangelista, W., & Souza Neto, J. (2015, February 9). COBIT 5 supports cloud computing migration in the Brazilian public sector. COBIT focus.

Gartner. (2012, March 27). Gartner says worldwide software-as-a-service revenue to reach $14.5 billion in 2012. Retrieved from http://www.gartner.com/newsroom/id/1963815

Gill, P. (2015). What is 'SaaS' (Software as a Service)? Retrieved from http://netforbeginners.about.com/od/s/f/what_is_SaaS_software_as_a_service.htm

Global Digital Infrastructure 451 Alliance. (May, 2015). Corporate cloud computing trends: Amazon leads a growing IaaS market, but Microsoft's Azure challenges.

Global Digital Infrastructure 451 Alliance. (November 2015). Corporate cloud computing trends: Cloud spending continues to outpace overall IT spending.

Hardy, Q. (2014, December 2). Computing goes to the cloud. So does crime. Retrieved from http://bits.blogs.nytimes.com/2014/12/02/computing-goes-to-the-cloud-so-does-crime/?_r=2

Kelly, H. (2012, August 7). Apple account hack raises concern about cloud storage. Retrieved from http://www.cnn.com/2012/08/06/tech/mobile/icloud-security-hack/index.html

Mitakos, T., Almaliotis, I., Diakakis, I., & Demerouti, A. (2014). An insight on e-learning and cloud computing systems. *Informatica Economica, 18*(4), 14-25. doi:10.12948/issn14531305/18.4.2014.02

Mohamed, A. (2009). A history of cloud computing. Retrieved from http://www.computerweekly.com/feature/A-history-of-cloud-computing

Mantelero, A. (2012). Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution. *European Journal for Law and Technology*, *3*(2).

Nieva, R. (2014, September 2). Revamped Google for work puts new spin on courting business. CNet. file://localhost/Retrieved from http/::www.cnet.com:news:revamped-google-for-work-puts-new-spin-on-enterprise:

National Institute of Standards and Technology (NIST). (2011). The NIST definition of cloud computing. [Special Publication 800-145]. 1-7.

Novak, J. D. (1998). *Learning, creating, and using knowledge: Concept maps as facilitative tools in schools and corporations*. Mahwah, NJ: Lawrence Erlbaum.

Perez, E. (2015, March 10). Sources: State Dept. hack the 'worst ever'. Retrieved from http://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/

Pershing, J. L. (2006). *Handbook of Human Performance Technology: Principles, Practice and Potential*. Los Angeles, CA: Pfeiffer.

Skidmore, S. (2013). *Mobile application management and employee training*. Retrieved from https://www.apperian.com/mam-blog/mobile-application-management-and-employee-training/

Svantesson, D. & Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review. (26). 391-397.

Wei, L., Zhu, H., Zhenfu, C., Dong, X., Jia, W., Chen, Y., Vasilakos, A. (2013). Security and privacy for storage and computation in cloud computing. *Information Sciences*. (258). 371-386.

Weinberger, M. (2015, March 12). Why 'cloud computing' is called 'cloud computing.' Business Insider. Retrieved from http://www.businessinsider.com/why-do-we-call-it-the-cloud-2015-3