Business Continuity Opportunities in the Cloud

A Small to Medium Business Perspective

Donald Zullick and Cihan Varol
Department of Computer Science
Sam Houston State University
{dhz001@shsu.edu, cxv007@shsu.edu}

***Abstract*—This research paper begins with a look at current work in business continuity as it relates to the cloud and Small to Medium Business (SMB). While cloud services are an emerging paradigm that is quickly making an impact on business, there has been no substantive research applied to SMB in disaster recovery efforts. Seeing this lapse, we have taken a fusion of continuity and cloud research with application to the SMB market. It is an initial reflection with base framework guidelines as a starting point for implementation. In this approach, our research ties together existing work and fills the gap with an SMB outlook.**

Keywords-business continuity; cloud services; medium size business; risk assessment; small business.

I. INTRODUCTION

Cloud services and related technologies are providing options to a proprietary, location based model that has dominated the industry for decades [1]. This has always been a challenging aspect for the Small to Medium Business (SMB) market. While this group is often one of the most important drivers in business activity, staffing is generally limited to operational functional units, most often this means a lack of dedicated technology personnel [2]. While this is by no means debilitating to normal operations as the SMB will hire staff for core functions as necessary, the situation has a distinct tendency to reflect limited or restricted technology resources.

The primary reason that cloud services can be a powerful differentiator for SMB's would be the "pay-as-you-go" model and only budgeting for the services you require [3]. Enterprise organizations are generally going to have complex infrastructure, staffing and potentially even continuity costs, which will fundamentally reduce the benefits of cloud services. In addition, the needs at the enterprise level will be greater along with associated costs. At the SMB level, it will generate additional costs but often will be a la carte so planning can be done, contracts put in place, and Service Level Agreements (SLA) signed which will assist in continuity preparedness. The primary reason this research is important and why it stands out is due to conventional wisdom dictating that enterprise solutions are applicable for all organizations, simply scaling down the implementation for the SMB. This is an erroneous assumption and dangerous to SMB technical operations and continuity planning.

This research took a look at conventional and enterprise level business continuity work that had been done previously [4][5]. After getting an understanding at that level, personal understanding of the SMB market has been utilized to interpret this information into a micro framework with flexibility to conform to the unique needs of the target organizations. While the result is not formally distinctive, which is the ultimate point of this work, the SMB businesses require a distinct overarching set of guidelines that can be applied to specific operational needs. The final output of this work is such a set of steps that can be used in a flexible manner yet have an open source aspect that can be customized to self-determined needs.

Rest of the paper is organized as follows: The second section will provide information about the cloud services and its usage. The third section provides background work on application of cloud services in disaster recovery / business continuity efforts. This is followed by the interpretation of how cloud computing takes a place in the SMB market. In Section 5, we will present a business continuity framework that can be used in SMB and the paper is finalized with a conclusion section.

II. ABOUT CLOUD SYSTEMS

A. Cloud Services

As covered by National Institute of Standards and Technology (NIST) (2009) [6], there are 4 types of cloud system consisting of public, private, hybrid and community as shown in Figure 1. The most popular and common one is the public cloud, though there are other alternatives as noted here if there are specific needs of an organization that cannot be met by a public option. This may come about from system needs or perhaps even from specific security needs. The primary scope of this research will center on the public cloud and the related potential offered by providers in this space.

Marston et al. [7] stated that accessing to a system independent of device and location represent a major shift in computing compared to all other previous techniques. There are some associated key advantages of this technology from lower cost to immediate access to hardware resources, while cloud resources potentially increase innovation with

 ISBN: 978-1-61208-345-2

availability for enterprises to scale their operations along with others [7].

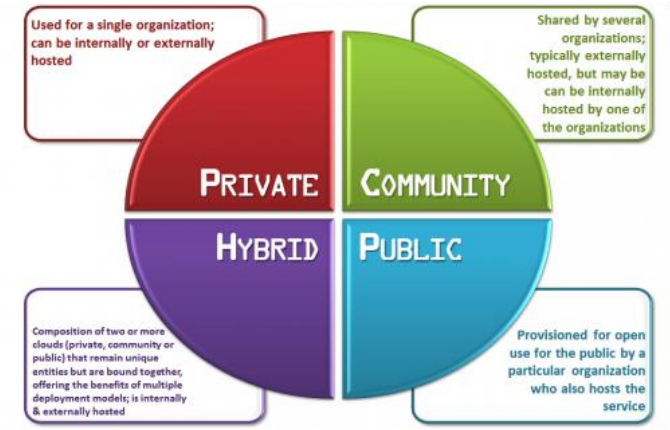

Figure 1. Types of Cloud Computing [3]

Some of the final elements of coverage on Cloud computing is the classification of services and applications. According to Lin and Chen [8], cloud services delivery models can be broadly categorized into four:

- Software as a Service (SaaS), in which applications are exposed as a service running on a cloud infrastructure.
- Platform as a Service (PaaS), programming platforms and tools (such as java [9], python [10], or .NET [11]) and/or building blocks and APIs for building cloud-based applications and services are made exposed as a capability.
- Network as a Service (NaaS) includes the provision of a virtual network service by the owners of the network infrastructure to a third party, and,
- Infrastructure as a Service (IaaS) resources (compute, storage, and network) are exposed as a capability.

Overall, cloud computing is the result of evolution and adoption of existing technologies and paradigms. So far, the descriptive information and the associated cost figures build up the fairly easily discernible benefits related to the cloud and stands out as a good potential structure to be used as IaaS in business continuity. That being said there are also security considerations to be assessed.

B. Challenges in the Cloud

There are challenges related to utilizing a framework that is so publicly available. A big part of the risk comes from having to access proprietary resources across a public WAN. While there will be established and implemented security protocols in place, with the escalating nefarious cyber activity, any additional exposure can be an increased risk.

Cloud computing inherently is affected by common and well-known Internet-based threats like Denial of Service (DoS) and SQL injections. Some of the security issues specifically related to Cloud computing [4] are:

- XML Signature Element Wrapping, renowned attack to web services
- Browser Security
- Cloud Malware Injection Attack, which tries to damage a spiteful service, application or virtual machine.
- Flooding Attacks, where the cloud is brazenly attacked
- Data protection
- Incomplete Data Deletion
- Locks in, affecting portability

C. Vulnerabilities

There are many potential vulnerabilities for cloud-based technologies and services, but they can be mitigated with an understanding of what types and categories are included. A place to start is the core cloud technologies, such as web based services, virtualized infrastructure as a service, and cryptography. Next essential characteristics are like services that are on demand, network access from anywhere, resource pooling and an elastic demand needs to be assessed. Within those areas is a further defined exploration of vulnerabilities along with security controls that can be implemented to provide mitigation [12]. The movement from proprietary infrastructures and technology provides a challenge in vulnerability assessment as it is difficult to define boundaries and responsibilities. This is where a solid review of the SLA comes in the picture.

It is not enough to be aware of options, risks and then just forge ahead hoping for the best. Even a small or medium sized business needs to stay viable, especially in a time of continuity threats. As the enterprise grows, being reliable and available can be some of the best tools in attaining and more importantly, retaining customer base goodwill.

Data and applications that are controlled and serviced internally can be readily assessed according to organizational protocols and security measures. Much like our customers trust us to be vigorous in protecting their data, housing assets in the Cloud implies an SLA. When it comes to the Cloud "the enterprise data is stored outside the enterprise in the most of Cloud Computing service model. Therefore, the Cloud Computing vendor is usually suggested to adopt additional security checks to prevent breaches [13]." The Cloud model implies a comprehensive enterprise model of availability and security. In order to rely on this model at a time of greatest need such as a continuity situation, there must be well established assurances. Ultimately, while the Cloud has revolutionized the computing environment there are a number of threats from the network to applications that need to be controlled. This will take effort from the enterprise utilizing the services through audits and to ensure that Cloud service providers are adhering to their SLA's [14]. In order to successfully leverage the cost and availability for a Small to Medium Enterprise, the security

 ISBN: 978-1-61208-345-2

concerns will need to be explored and accounted for prior to establishing Cloud services as a continuity option.

III. LITERATURE REVIEW: CLOUD SERVICES IN DISASTER RECOVERY

Although cloud-based business process has been discussed widely and adopted by several companies, there is only a few study reflect the usability of cloud services for business continuity purposes.

Wood et al. [4] discussed about applicability of cloud in disaster recovery effort. Overall, the authors showed that warm backup sites can take the most advantage of the cloud's pay-as-you-go pricing model, since a hot backup site will be costlier. Their research also showed that cloud services can offer customers up to 85% cost reductions compared to company-owned equipment in business continuity.

According to Creeger [5], cloud services reduces the cost significantly. By enabling virtual machines to be sent to the cloud for access only when needed, virtualization becomes a cost-effective disaster recovery mechanism. Typical business continuity effort costs are twice the cost of the infrastructure. With a cloud-based model, true disaster recovery is available for an approximate of 5 percent extra cost for the company, a significant savings. Additionally, because external cloud service providers replicate their data, even the loss of one or two data centers will not result in lost data. Although the cost benefit is obvious, the authors stated most SMBs make no investment in disaster recovery via cloud.

As mentioned earlier, security within the cloud has been an issue because the business is giving up control of their data to an external entity. This issue is compounded by the fact that the data can be located in multiple locations making it very difficult to track. However, Alhazmi and Malaiya [15] suggested that there is some evidence with proper security protocols and policies that these issues can be addressed even if cloud is used for business continuity purposes. They also stated that with public cloud vendors, a higher security level can be achieved because they can employ more security personal that can monitor access of the data and if there is a breach, it has higher probability of being reported and stopped faster than a private cloud system.

As reflected from above, the work on cloud systems in disaster recovery efforts are limited and also the built frameworks are not considering the size of the company. Therefore, this work in using cloud services in business continuity from small size to medium size business will be unique in terms of what it proposes.

IV. SMB BUSINESS CONTINUITY AND THE CLOUD

A. SMB Market and Services

The challenge has always been greater for technology and related implementations in an SMB beyond even just plain economics. Staff levels are going to be limited to the levels of primary functional ability. There is not a scenario where there can be specific, targeted teams for assessment, testing or ultimately deployment on demand. Even though the SMB market is recognized to be a powerful driver of business activity on a macroeconomic level, anything other than enterprise organizations have often been overlooked. It is an exponential degree of greater difficulty to provide external services and consulting for the SMB market.

This exploration is specifically in the area of business continuity planning, but the challenges inherent to the scale of business for the SMB market are apparent in all level of functional aspects. As a whole, the potential market and revenue generation is rival to enterprise businesses, but the value has to be extracted in a dispersed and relatively scaled per business microeconomic manner. No million dollar consulting engagements to be had in this group.

There are services that have become available to the SMB market in recent times along the lines of the most readily apparent cloud services, but there are also innovative companies in industry that provide greatly needed and appropriately targeted consulting, such as HourlyNerd [16]. Taking advantage of an obvious business need and the glaring lack of services provided in this arena, HourlyNerd meets a need by providing affordably priced MBA guidance recruited from top business schools such as Harvard and Northwestern. Some of the obvious advantages of HourlyNerd are that the members are all from top 20 universities in the United States or elite international institutions, they have had their backgrounds thoroughly checked during the admissions process and have the requisite networks, resources and solutions.

B. Business Continuity

In the business continuity process, the SMB will not have the same resources to apply for planning, testing or ultimately application in time of need. Often there will be few, if any, specific technology resources available for any stage of the process. This is where an organization needs to be creative within the expanding boundaries of technology services that in practice actually have a greater impact on the bottom line for an SMB than for an enterprise scale business. Cloud technologies can provide a solid infrastructure and specific applications such as readily available Google Docs [17], technology can be leveraged in an extremely economical and flexible manner. The greatest hurdles would come from simple adoption arising from lack of understanding of available options. Accordingly, this is the point of the process where previously mentioned HourlyNerd could be instrumental in relatively priced enterprise scale planning and services at the SMB level.

C. Power of the Cloud

Some specific cloud-based and cloud-related technologies that can be powerful enablers for the SMB are not only the clearly defined cloud based services, but another organizational paradigm that can tie in to this movement and be leveraged for business continuity is Bring Your Own Device (BYOD). As the business stalwart PC

 ISBN: 978-1-61208-345-2

sales continue to experience a precipitous fall, as consumers opt for the tablet and smartphone options, this trend is one that is favorable to the SMB market. In a continuity situation, communications are fundamental to any situation. Ready adoption of employee driven trends of BYOD and integration into operations can be a differentiator for smaller organizations without a dedicated technology budget or staff.

By having a policy that supports the adoption of mobile devices along with company-based reimbursement, an SMB could support adoption of business continuity ready devices and technologies without the requisite corporate investment or commitment of resources. Employees that embrace this trend are more likely to be self-trained and have a reliable and useful level of home based connectivity. Encouraging the adoption by providing company support, the investment can be compounded in potential benefit in times of need. This can help increasing the likelihood of employees having an understanding at least, and a level of comfort at best with the cloud based services that can make or break a continuity process at a SMB.

D. Security Concerns

Concerns are the same at this level as it is at any level and that is related to security, more specifically to cyber security. Cybercrimes and attacks are a very prevalent threat to business and government continuity. Verizon recently, released a report showcasing some disconcerting facts and figures on how small businesses are the easiest prey for cybercriminals [18]. “Of the 621 confirmed data breach incidents Verizon recorded in 2012, close to half occurred at companies with fewer than 1,000 employees, including 193 incidents at entities with fewer than 100 workers. A separate report from cyber security firm Symantec confirmed that trend [19]. It found cyber-attacks on small businesses with fewer than 250 employees increased 31% in 2012, after growing by 18% in the prior year.” It is an ongoing continuity situation for the SMB market, building on previously mentioned factors such as lack of dedicated technology staff and funding. These elements need to be a part of the business continuity planning as it constitutes a threat to the organization

V. SOLUTION

Now, that we have explored the situational factors, concerns and how cloud services with related technologies can be solution facilitators, we need to look at a formalized exploration of a framework.

Three risk management methods EBIOS [20], NIST 800-39 [21], and IT-Grundschutz [22] are well-known and widely adopted techniques. Although these methods have been widely recognized, these methods fit for large scale businesses [23]. While implementation of the methods to smaller organizations is possible, it will introduce greater cost and a potential of information redundancy if viewed from “information-as-needed” point of view. By studying these methods, we derived that their processes are widely different and the quantity of sub-process/sub-steps may vary which adds to the complexity and cost to perform these steps for smaller organizations. Also, we observed that some of them possess useful processes that can be useful for smaller businesses or organizations while they may also lack in other parts of processes. For example, while EBIOS does not possess the concrete post-implementation monitoring strategy and evaluation, as showcased by NIST 800-39, it does, however, do initial study of existing security measures, which is not included in NIST 800-39.

Based on the analysis, as shown in Figure 2, a combination methods of Context Study from EBIOS, Knowledge catalogue concept from IT Grundchutz, and Continuous Risk monitoring and evaluation from NIST-800-39 can be combined to be used in Risk Management in Cloud computing for SMB business.

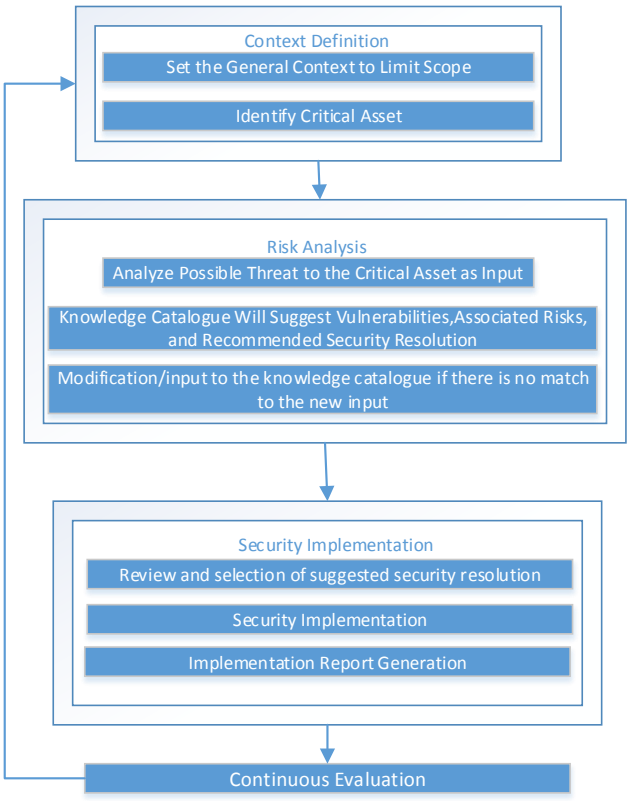

Figure 2. Proposed Risk Management Method Process

- Context Definition: First stage is the context definition. In this stage the person/team will define the context of the recovery plan to limit the scope. The other main activity will be the identification of critical assets of the business.
- Risk Analysis: Once the context definition is done, analysis of any possible threats to cloud that can affect the critical assets need to be listed as a list of inputs. These inputs are then compared to the knowledge catalogue to see if there are any existing similar threats from which can be derived its vulnerabilities, associated risks, and recommended

 ISBN: 978-1-61208-345-2

security resolution/controls. If there are no matches of the inputs in the knowledge catalogue, further risk assessment will be done to define vulnerabilities, associated risks, and recommended security resolution/controls. This can become a basis for future risk analysis.

- Security Implementation: From the risk analysis, the risk assessment report will provide the list of risks and recommended security resolutions/controls in cloud. With the Cloud Controls Matrix (CCM) guideline available from Cloud Security Alliance (CSA) that is specifically designed to offer fundamental security principles in cloud [24], the stakeholder (usually business owner) can then decide which controls they want to be implemented and a report documenting the implementation along with the list of any risks that are not controlled due to acceptance from the stakeholder need to be generated.
- Continuous Evaluation: The cloud environment is one of ongoing change and to properly address a plan or potential implementation, there should be periodic assessments and monitoring on a regular basis. As understanding grows along with adoption of cloud based business practices and the associated risk assessment, an organization needs to treat this as a living process and revisit the framework, applying modifications as deemed necessary.

As shown in Figure 3, BYOD tied in to cloud services can provide communications, data, and applications capabilities. Besides cost advantages to the companies, BYOD can improve the agility and productivity of work practices amongst employees in an enterprise [25]. Prohibiting personal devices in a business recovery effort is risky, since employees may be forced to use their own devices because of lack of secured devices after a disaster. With the introduction of BYOD, the devices are owned by the individuals not by the companies. The device may be managed both by the company and the user as well. Accountability is not something that goes away for a user just because they personally own the device. At the end, the data belongs to the company.

The suitable defense in securing BYODs begins with the same requirements that are applied to devices that are already owned by the business. These security measures include:

- Enforcing strong passcodes on all devices. By password protecting the devices, a user acknowledges accountability and responsibility for protecting their data.
- Antivirus protection and data loss prevention (DLP)
- Full-disk encryption capability for cloud storage
- Mobile device management (MDM) to wipe important data when devices are lost or stolen
- Application control. The device should be able to perform other daily needed jobs when not in use for recovery efforts.

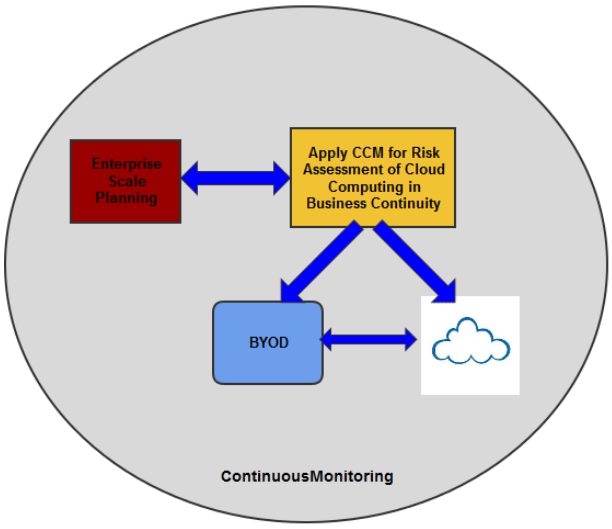

Figure 3. Framework for Business Continuity in Small Business

VI. CONCLUSION

There is great potential for the SMB market when it comes to cloud services. The challenge does not change but the impact of the solutions, and the related value of those solutions is much greater. A Small to Medium Business can have an as needed infrastructure that can be leveraged on an ongoing, day to day basis but beyond that can have an accessible infrastructure able to scale up or out in a time of distress. For this type of implementation, the costs of compliance often have a greater impact due to the smaller economies of scale, yet at the counterpoint cloud services offer a greater positive impact due to the scalable implementation and usage based pricing and services.

With some planning and a reasonable investment, an SMB can now achieve a level of risk assessment with associated mitigation by making the most of emerging offerings, such as the cloud, BYOD and companies like HourlyNerd. The current business environment is very challenging for everyone, at times debilitating to smaller enterprises and the ability to take advantage of these powerful, differentiating services and paradigms can give a SMB a good toolbox to build a future.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145 (September 2011). National Institute of Standards and Technology, U.S. Department of Commerce, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [retrieved: March, 2014]

[2] D. Greenberg, B. Barringer, and G. Macy, "A qualitative study of managerial challenges facing small business geographic expansion," Journal of Business Venturing, vol. 11, issue 4, July 1996, pp. 233-256.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communication of the ACM, vol. 53, issue 4, April 2010, pp. 50–58, doi:10.1145/1721654.1721672

 ISBN: 978-1-61208-345-2

[4] T. Wood, E Cecchet, K. K. Ramakrishnan, P. Shenoy, J. Van der Merwe, and A. Venkataramani, "Disaster recovery as a cloud service: economic benefits & deployment challenges", Proc. 2nd USENIX conference on Hot topics in cloud computing (HotCloud'10), June 22-25, 2010, Berkeley, CA, USA, pp. 8-8.

[5] M. Creeger, "Cloud Computing: An Overview," Queue – Distributed Computing, vol. 7, issue 5, June 2009, pp. 1-5.

[6] S. Qaisar and K. F. Khawaja, "Cloud Computing: Network/Security Threats and Countermeasures," Interdisciplinary Journal of Contemporary Research in Business, vol. 3, issue 9, January 2012, pp. 1323-1329.

[7] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang and A. Ghalsasi, "Cloud computing – The business perspective," Decision Support Systems, December 2010, pp. 176-189.

[8] A. Lin and N. Chen, "Cloud computing as an innovation: Perception, attitude, and adoption," International Journal of Information Management, April 2012, pp. 533-540.

[9] Java, http://www.java.com/en/, [retrieved: November, 2013]

[10] Welcome to Python.org, https://www.python.org/, [retrieved: November, 2013]

[11] Microsoft .Net, http://www.microsoft.com/net, [retrieved: November, 2013]

[12] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security & Privacy. March-April, 2011, pp. 50-57.

[13] C. Ku Fan and T. Chen, "The Risk Management Strategy of Applying Cloud Computing," International Journal of Advanced Computer Science and Applications, vol. 3, no. 9, 2012, pp. 181-191.

[14] R. Bhadauria and S. Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," [Online] Available: http://arxiv.org/ftp/arxiv/papers/1204/1204.0764.pdf [retrieved: November, 2013]

[15] O. H. Alhazmi and Y. K. Malaiya, "Evaluating Disaster Recovery Plans Using the Cloud," in Reliability and Maintainability Symposium, Orlando, FL, 2013, pp. 1-6.

[16] L. Lavelle, MBA's: Why Hire When You Could Rent by the Hour? [Online] Available: http://www.businessweek.com/articles/2013-04-11/mbas-why-hire-when-you-can-rent-by-the-hour [retrieved: November, 2013]

[17] Google Docs (Drive), [Online] Available: http://drive.google.com/?utm_medium=et&utm_source=about&utm_campaign=et-about [retrieved: November, 2013]

[18] P. Kavilanz, "Cybercrime's easiest prey: Small businesses", [Online] Available: http://money.cnn.com/2013/04/22/smallbusiness/small-business-cybercrime/index.html?iid=Lead [retrieved: November, 2013]

[19] Symantec, www.symantec.com [retrieved: November, 2013]

[20] ANSSI, "Expression of Needs and Identification of Security Objectives: EBIOS Method of RIsk Management," ANSSI: Paris, France, http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html [retrieved: November, 2013]

[21] N.Hunstad, "The Application of NIST Special Publication 800-39 for Small Businesses and Organizations" ,M.Sc. Thesis, UMN, MA, 2011, http://www.nathanhunstad.com/docs/NathanHunstadCapstone800-39Public.pdf [retrieved: November, 2013]

[22] IT Grundschutz Methodology, BSI - Standard 100-2:200. [retrieved: March, 2014]

[23] S. Antolík, "Risk Analysis in Information Security and Tools Used for Risk Analysis," ARSA 2012, Proceedings in Advanced Research in Scientific Areas, The 1 st Virtual International Conference, EDIS – publishing institution of the University of Zilina, December 3-7, 2012, pp.1906-1911.

[24] E. de Souza, S. Cordero, and T. Kenyon, "Cloud Controls Matrix (CCM)", [Online] Available: https://cloudsecurityalliance.org/research/ccm/ [retrieved: March, 2014]

[25] W. Keith, J. V. Miller, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," IT Professional, vol. 14, issue 5, September-October 2012, pp. 53-55, doi:10.1109/MITP.2012.93

 ISBN: 978-1-61208-345-2