# SOME SMEs DATA SAFETY AND SECURITY ISSUES IN THE IN-HOUSE AND IN THE CLOUD COMPUTING

**Zoran Čekerevac**[*]
**Savo Radonjić**[**]

## ABSTRAKT

Článok prináša analýzu o potrebách malých a stredných podnikov pre ukladanie dát a spracovanie, a riziká, ktoré sa môžu objaviť pri použití cloud ako miesto na plnenie svojich potrieb. Porovnávacia analýza o rizikách používania cloud a in-house technológií je uvedený spolu s niektorými príkladmi. Osobitná pozornosť je venovaná problematike ochrany proti rizikám na internete strane poskytovateľa: hakovanie a dohľad.

Na konci práce sú uvedené niektoré odporúčania pre malé a stredné podniky vo vzťahu k cloud computingu.

**Kľúčové slová**: cloud computing, bezpečnosť dát, zabezpečenie dát, ochrana dát, malých a stredných podnikov

## ABSTRACT

The article presents an analysis about SMEs' needs for data saving and processing, and risks that can appear when using cloud as a place to fulfill their needs. A comparative analysis about risks of using cloud and in-house technology is given together with some examples. Special attention is paid to the problems of protection against risks on the Internet provider's side: hacking and surveillance.

At the end of the work, some recommendations for SMEs in relation to cloud computing are given.

**Key words:** Cloud computing, data safety, data security, data protection, SME

[*] Zoran Čekerevac, PhD, Assoc. Prof., Faculty of Business and Industrial Management - „Union“ University Belgrade, Kneza Višeslava 27, 11000 Belgrade, Tel. +381 (11) 823 24 27 and Business School ''Čačak'' in Belgrade, Gradski park 2, 11080 Beograd-Zemun, Tel. +381 (11) 377 15 52, e-mail: zoran.cekerevac@vpscacak.edu.rs

[**] Savo Radonjić, PhD, Docent, Business School ''Čačak'' in Belgrade, Gradski park 2, 11080 Beograd-Zemun, Tel. +381 (11) 377 15 52, e-mail: savo.radonjic@vpscacak.edu.rs

# 1 INTRODUCTION

The official position of the European Union in relation to the prosperity of its citizens is that it just depends on the development of small and medium-sized enterprises. This is not surprising, given that out of the 19.3 million enterprises in Europe in the year 2001, 99.8 percent were small and medium-sized enterprises, employing 66 percent of the total active population, and contributing by 54 percent to total generated turnover [1]. In 2009, in EU-27 were 20,791,190 enterprises with the SMEs[1] participation of 99.8%, same as eight years before [2]. That is why SMEs are recognized as the backbone of EU economy.

Different forms of e-businesses play an important role in the business of SMEs. If the company's dependence on the data is considered, it can be seen that in that respect it is completely irrelevant whether it is a large multinational company or a company of ten employees. Both depend on the data they use in their daily work. Problems can arise either because of the banal loss of power supply, PC-theft, malicious hacker intrusion, virus attacks, but also because of the massive disasters that may be caused by floods or earthquakes as it was in March 2011 in Japan. SMEs take considerably small care of measures for their safety, and many of them find that they are not interesting to attackers, and that attacks will miss them. [3] Normally, this assumption is totally unwarranted.

SMEs tend to have all their critical data on a single server. If the server "crashes", because most offices depend of that server, it would have to be running and to be fully restored immediately. Otherwise, the whole system could be exposed to costly consequences. SMEs and, also, large corporations, in regulated economies, are subject to the same requirements in the terms of quality and data availability, and, also, data protection. In the United States, there are established sets of very specific rules about the availability, organization, and regulatory data protection laws, such as: HIPAA, DOD 5015, FDA Part 11, Sarbanes-Oxley, SEC Rule 17th ... [4], and very severe penalties are provided for violations. The problem of SMEs is the lack of funds to undertake necessary measures. In addition, any disruption in cash flow is often fatal for SMEs. Aidan McDermot estimated in his article "A Small Business Approach to Computer Downtime" [5], that incidents can cost a small business from $232 to $844 per PC, depending of the kind of incident, as it is shown in the table 1.

*Table 1 An example of downtime cost (Authors presentation of the data in [5])*

| Option | Total downtime | Lost wages | Cost of service | Total cost of downtime per PC |
|---|---|---|---|---|
| Onsite service | 8 hours | $36.20x8=$289.60 | $200 | $489.60 |
| Drop off service | 20 hours | $36.20x20=$724 | $120 | $844 |
| Remote service | 2 hours | $36.20x2=$72.40 | $160 | $232.40 |

[1] SMEs are defined by the European Commission as having less than 250 persons employed. [2]

Although the leadership of SMEs can find it difficult to refute the importance of preparing for operations in emergency situations, it is easy for them to postpone the planning and implementation of measures for crisis situations because of everyday problems and limited resources. US Small Business Administration (SBA) estimates that 25 to 40% of small companies disappear after a crisis or a prolonged suspension of operations. Companies, that are not able to resume their operations in 10 days of a disaster, are not likely to survive [6]. According to the same source:

- 80% that do not recover from a disaster are likely to go out of business within one month
- 51% of companies close within two years
- 75% of business without a business continuity plan fail within 3 years of disaster
- 43% of business never reopened

Although the first thought of the SME leadership is the selection of appropriate technology, the first step in data protection should always be the selection of the right people, policies and procedures. The person responsible for data protection, at the very beginning of his work, has to organize a small group that is fully familiar with the technology of business. It is a way to determine the actual needs and possible critical places in the system.

## 2 DATA PROTECTION STRATEGIES

To create comprehensive and effective strategy for data protection is serious job. Data protection is connected with many challenges, with technology, but also with standards and compliances, the changes in way of doing business, up to the every single person which is in touch with sensitive data. There are priorities that should be set. It is necessary to define potential and likelihood points of data endangerment, to focus on situations where interventions are the most expected. It is impossible to remove all risks, but strategies must be good enough to moderate serious risks. They need to prepare individuals to react in crisis situations, and provide them tools that will allow correct decision making.

One of the first steps in any of data protection strategies measures for data protection is data backup. The need for backup is cowered also by legislation and privacy laws. The last years appeared a great number of state and local laws and regulations regarding data storage and privacy. Much of this has been driven by identity theft as well as the unintentional posting of sensitive data on the Internet. [7] Backup plan should be clear, specific and easy to follow and should cover all SMEs data protection needs. The data should be backed up on regular intervals, and the frequency of backups depends of the size and nature of business, number of computers and their location, amount of data, but also whether the SME maintain normal or 24/7 business hours. The second part of data protection strategy should cover archive, and, the third, data recovery.

Finally, strategy should establish a periodic system testing schedule. Many a company has needed to restore data, but only discovered the backup media is corrupted or blank. [7]

One of the most important parts of the data protection strategy is a decision about the way of data keeping and processing:

- In-house data keeping and processing, or
- Cloud computing.

Luckily, there are multiple choices that can lower costs and increase business agility, including server virtualization, internal and external private clouds, and public clouds. [8] In any case, a company must think about storage automation which can deliver the availability, performance and data protection required by users. The automatization can reduce resource requirements, lover provisioning costs and increase service level up to 80%. [9]

## 2.1 IN-HOUSE DATA KEEPING AND PROCESSING

When the budget is defined, it is possible to choose a technology for data storage. It is easy to conclude that not all technologies are equally good for all SMEs. Due to differences in methods of data storage, data access, durability of the medium on which the data are stored, the speed of receipt and delivery of data, prices and other factors (e.g. mode of business operation: one or more locations), appropriate technology should be chosen very carefully. For in-house data keeping and processing, a company can apply own servers, including server virtualization which allow the server administrator to divide one physical server into multiple isolated virtual environments using some software application. Also, a company can use internal private storage clouds that can ensure that information remains safely within the company under the IT department’s security parameters while providing the necessary storage capacity across the enterprise. [9]

At companies operating in multiple locations, use of magnetic tape backup on the place of use may be the solution if the company has staff trained to wipe and maintain tape, to store them properly, to copy them regularly, and, if necessary, perform system recovery. Hence, it is necessary to ensure proper discipline and appropriate regularity in the work. SMEs face a big dilemma [3]:

- **Tapes as a backup systems** are fairly inexpensive and reliable, but offer modest capabilities in terms of DRA and ADL for critical applications. They are mostly ineffective for remote locations.
- **Hardware mirroring**, that uses remote copy technology to provide synchronous mirroring between two locations, offers excellent DRA but can be overly expensive solution for SMEs. In addition, this solution is far from ideal for backing up from remote locations that, often, are associated with low-bandwidth connections. Hardware mirroring requires huge data flows between sites.

Solutions based on software-based asynchronous replication can be cost effective for SMEs in terms of ADL for critical applications. Thereby, the complexity and high cost of synchronous replication are avoided. With software-based replication, only the bits that were changed during data processing are changing.

Even data stored in-house, in the own premises are not safe, because there are always the risks. From data theft, eavesdropping and unauthorized copying, up to the theft of physical hard disks. For protection against hackers, there are a number of measures, but the question is whether the SMEs are able to recognize and use them. The reasons are primarily in the SMEs staff potential. Additional risk can appear from possible natural disasters, fires and similar unwanted events.

Although the organizations take care about their data, they are mainly focused on external threats. But, there are also internal threats, mainly from permanent staff, former workers and employees in cooperative companies. The staff and especially careless workers are probably the biggest threat. They have daily access to sensitive information and for misuse they often do not need high levels of education. Also, big threats can be caused by former workers, regardless of whether they were dismissed or were changed their job to another (especially in competitive) organization. Subcontracting companies can be a big problem for security systems because they often have access to sensitive data. In the area of personnel management it is necessary to apply all available measures to meet the threat of destruction, damage and stealing information. If not completely eliminated, they should be, at least, reduced to acceptable limits by: the selection of personnel; working adaptation; and for security education and training. Each measure must be carefully analyzed and fully applied. Also, nonetheless, a system of passwords and privileges must be used.

## 2.2 CLOUD DATA STORRAGE AND PROCESSING

According to the Dictionary.com, the term “cloud computing” represents: “Internet-based computing in which large groups of remote servers are networked so as to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources.”

SMEs in recent years increasingly used cloud computing and stored data on servers in the cloud. The main reasons lie in the reduced need for maintenance of data and systems, improved Internet connections and low costs. In addition to these, there are other benefits such as: increased data security with the absence of the need to store data in remote locations, which, because of the risks connected with data storage in one place, until now imposed as an imperative. 35% of SMEs in 2012 signed up to use Cloud Computing Software. [10] But, there are also some security fears that hamper SME's cloud lift-off. SMEs can fear of cloud computing for two important reasons:

- Security of data transmission over the network, and
- Data security in place to keep.

Although there is always a risk, when use a secure line and encrypted data transfer, a company can consider that the data are secure. When the data are stored on the hard drive in the cloud, data are exposed to possible attacks. Big cloud providers are obvious and prominent targets for hackers. For example, in June of 2011, Melbourne based hosting provider Distribute.IT was subject of a targeted attack by an unknown instigator rendering data from four of its servers completely unrecoverable. [10] Even, if that risk is minimized by appropriate measures, the problem of the data safety can appear from the cloud data storage service providers. Assuming that none of the provider's employees will abuse the data access, there remains a risk of external pressures on provider to submit reports of the stored data to the governing structures and intelligence. A paper published in Document Management News [11] states that service providers can store data on someone else's servers, in other countries in which there are other laws in use, and that data owners have no information about it. For example, the European providers can keep data in the U.S. Thanks to the Patriot Act, foreigners are mostly unprotected in the USA because restrictions in law enforcement agencies' gathering of intelligence within the United States are significantly reduced. In his speech posted on YouTube Julian Assange [12] said: “There’s not a barrier anymore between corporate surveillance, on the one hand, and government surveillance, on the other.”

## *3 CONCLUSIONS - WHAT SME CAN DO TO PROTECT ITSELF?*

As it was mentioned, SMEs must define their data protection strategies, and decide about the platform for data keeping and processing. In choosing whether to use in-house, cloud or some hybrid solution, SMEs will have to prepare appropriate procedures to educate and train their employees, and fully apply planned measures including regular testing of hardware, software and procedures.

In the future, SMEs will generate huge amount of data and for their storage they will use cloud disks. Software resources will be available on Internet in the form of network versions and the most of jobs will be done in the cloud. To prepare themselves SMEs should follow some recommendations in relation to cloud computing that are well described in the OPC Guidance Documents [13]. They have to:

- Limit access to the information and restrict further uses by the provider;
- Ensure that the provider has in place appropriate authentication/access controls;
- Manage encryption;
- Ensure that there are procedures in place in the event of a personal information breach or security incident;
- Ensure that there are procedures in place in the event of an outage to ensure business continuity and prevent data loss.
- Ensure periodic audits are performed; and
- Have an exit strategy.

It is obvious that ICT sector is poised for strong growth of cloud services in the years to come, and SMEs will have the full access to the benefits, risks, and implications for privacy before using a cloud computing solution.

## BIBLIOGRAPHY

[1] *Mala i srednja preduzeća - Halo pomoć.* **Žarković, Zorica.** [ed.] Predrag Ursić. 33, Beograd : Evropski pokret u Srbiji, May 2001, Evropa Plus, pp. 6-7.

[2] **Eurostat.** Small and medium-sized enterprises. *eurostat.* [Online] European Commission, 12 14, 2012. [Cited: 04 09, 2013.] http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Small_and_medium-sized_enterprises.

[3] *Data protection in small and medium sized enterprises.* **Čekerevac, Z, Andjelić, S and Radović, D.** Novi Pazar, Serbia : Interbational University Novi Pazar, 2011. PROCEEDINGS of International Conference "Smal and Medium Enterprises – Possibilities and Perspectives 2011". 978-86-84389-26-0.

[4] **Wilson, Jean.** Oracle® Universal Records Management - Records Manager DoD Edition User Guide. *Oracle documentation.* [Online] 10g Release 3 (10.1.3.3.0), 03 2007. [Cited: 04 10, 2013.] http://docs.oracle.com/cd/E10316_01/urm/urm_doc_10/documentation/addons/user_recordsmanager_10en.pdf.

[5] **McDermot, Aidan.** A small business approach to computer downtime. *Ezine @rticles.* [Online] 01 11, 2006. [Cited: 04 10, 2013.] http://ezinearticles.com/?A-Small-Business-Approach-To-Computer-Downtime&id=126676.

[6] **Bolt.** Small business & natural disasters - Small business survival guide. *Bolt insurance agency.* [Online] 2011. [Cited: 04 05, 2013.] http://www.submitinfographics.com/full-size-infographics/Bolt-Small-Business-Natural-disasters-infographic-large2.jpg.

[7] *Developing an effective data protection strategy.* **Kherif, Nordine.** [ed.] Jill Franklin. Orem, Utah : Carlie Fairchild, 08 24, 2004, Linux journal.

[8] **Claybrook, Bill.** Cloud vs. in-house: Where to run that app? *Computerworld.* [Online] March 01, 2010. [Cited: 03 23, 2013.] http://www.computerworld.com/s/article/9162542/Cloud_vs._in_house_Where_to_run_that_app_.

[9] *Keeping Data In-house: Leveraging the Power of Storage Automation.* **Rhymes, Brent.** Alpharetta, GA : s.n., December 18, 2012, Data CenterJournal.

[10] *Small an medium sized enterprises data seccurity in cloud computing.* **Čekerevac, Zoran.** Chernivtsi : Bukovinsky Universitet, 2013. 978-617-614-028-3.

[11] **Reporter, Staff.** EU research points SMEs to data protection risks when using overseas cloud computing providers. *Document Management News.* [Online] 2012. [Cited: 02 10, 2013.] http://www.documentmanagementnews.com/the-news/software-as-a-service/232-eu-research-points-smes-to-data-protection-risks-when-using-overseas-cloud-computing-providers.html.

[12] **Assange, Julian.** EXCLUSIVE: Julian Assange on WikiLeaks, Bradley Manning, Cypherpunks, Surveillance State. [interv.] Amy Goodman. *EXCLUSIVE: Julian Assange on WikiLeaks, Bradley Manning, Cypherpunks, Surveillance State.* London : JouTube, 11 29, 2012. Transcript.

[13] **OPC.** OPC Guidance Documents: Cloud Computing for Small and Medium-sized Enterprises: Privacy Responsibilities and Considerations. *Office of the privacy commissioner of Canada.* [Online] 06 14, 2012. [Cited: 02 20, 2013.] http://www.priv.gc.ca/information/pub/gd_cc_201206_e.asp#toc9.

Článok recenzovali dvaja nezávislí recenzenti.