DATA PROTECTION IN SMALL AND MEDIUM SIZED ENTERPRISES

Zoran Čekerevac[1], Svetlana Anđelić[2], Dragan Radović[3]

1. Faculty of Industrial Management Kruševac "Union" University Belgrade, Serbia
E-mail: zoran.cekerevac@hotmail.com

2. Railway College of Professional Studies Belgrade, Serbia
E-mail: svetangela@gmail.com

3. Faculty for Management, "Alfa" University, Novi Sad, Serbia
E-mail: drarad@open.telekom.rs

Abstract

Like the large corporations, small and medium-sized enterprises (SMEs) rely on storage of their important data on their own servers. Limited resources and vulnerability to intrusions, bring the small and medium-sized enterprises at greater risk. The reliance of small and medium-sized enterprises on the classic backup of their servers may be an adverse decision in the recovery plan for sudden disasters. Basic backup provides protection to a small extent. Periodically recording data to a backup tape or disk may endanger SME's data and may lead toward the loss of time in unacceptable quantities. A prerequisite for a speedy recovery and return into the operational state is a comprehensive disaster recovery plan, which includes quick access to copies of the data that are constantly updated by the so-called system "up-to-the-minute copy". The paper discusses measures that SMEs can and should take to protect data, including cloud-based solutions. Special attention is paid to the choice of data storage technologies and ways to simplify data protection.

Key words: Small and medium sized enterprises, data protection, crisis management, technology, cloud-computing, Internet

JEL codes: L26, M15, O33

1. INTRODUCTION - DEPENDANCE ON THE DATA

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]*. There is no doubt that small and medium sized enterprises and entrepreneurs (SMEs) have become an important lever of economic development of Serbia. Now the "small business" exercise for about two-thirds of total turnover and about 60 percent of gross added value. This sector has offered in previous years, most new jobs and in 2010 the age was recruited 67 percent of all employees in the economy. SMEs have absolute predominance in the total number of businesses. Of the approximately 333,500 of all registered companies, operating in Serbia in the year 2010, this group accounted for 99.8 percent*[2]*.

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 lose 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. Small and medium sized enterprises (SMEs) take considerably small care of measures for their safety. Many SMEs find that they are not interesting to attackers, and that attacks will miss them. This assumption is totally unwarranted, because "every commodity has its own customer". Large companies that heavily use the Internet, and base their businesses on it, are usually exposed to comprehensive and more sophisticated attacks, but, also, the attackers beginners have to start somewhere, for example by attacking less-protected systems, where they have a realistic chance to achieve their aims. This is the reason why management of SMEs must not see the protection as the protection from a hypothetical and a little probable attack. The problem must be approached with the whole necessary seriousness. The holes once left in the protection may later prove to be very painful and expensive. Although the problems of hardware protection and protection of supply interruption are now easily solvable, even this aspect should not remain neglected.

Culture of conducting business in today's conditions is significantly changed from the recent past, so the risks are changed. New factors of doing business require monitoring and analysis of growing amounts of data, including an increasing number of different data that becomes critical in the business.
In addition, consumers do not tolerate long interruptions in the business of a company. In cases when the doing business with a company, which has downtime, become uncomfortable, consumers turn to other companies that work without interruptions. Normally, the acceptable duration of interruptions in the work are not always the same. If computer user waits for an answer for more than three seconds, or gets messages like *"The server is busy. Please try later!"*, he sees them as hardly acceptable, and if repeated, will try to find an alternative solution.

Today's challenges in the field of data protection represent a significant risk for companies of all sizes, but small and medium enterprises are exposed to the biggest risks. SMEs often have no staff or budget to provide an acceptable recovery. Often, there is no recovery plan, there is no site recovery, or backup to a recovery site is not far enough from the primary location in case of natural disasters.

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, they are subjects 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 ...*[3]*, and very severe penalties are provided for violations. In Serbia, legislation of this kind is still in its infancy, but here there are existing laws: the Law on Electronic Commerce, the Law on Protection of Personal Data ... 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. In his article "A Small Business Approach to Computer Downtime", Adian McDermot estimated that each incident can cost a small business between $ 200 and $ 800 per incident, and PC. *[4]*
Microsoft® Windows® Small Business Server (SBS) allows, to a limited extent, to small businesses to use many functions that also large companies use:

- basic network services: DNS, DHCP,..., SSH;
- Windows networking: files and printers sharing;
- Web server;
- FTP services;
- e-mail server, and, optional, database server;
- support for mobile devices, as well as
- backup and restore functions.

Linux Small Business Server (LSBS) offers many of the same services as Microsoft® Windows® Small Business Server, but, also, offers the Wiki as a document management system, as well as advanced networking tools - Nagios, Nessus and Nmap.

SBS and LSBS, they make available tools to create periodic backups. However, relying on the built-in basic backup, to protect all bases in an emergency or disaster, can leave work damaged due to potential gaps in protection.Tapes and disk backups can only return data to the point of the last good backup, which probably was the end of the previous day. All data entered since the last good backup will be lost. If the most recent backup is incomplete or damaged, then the previous in order backup will be used. That will cause a loss of even more data and so on. Server recovery by using the backup copy is shorter than the

time of normal operations re-establishing, because the data can be returned from the backup media to the user's disk so it can be used.

In the development of small businesses it is always necessary to be optimistic to achieve favorable results, but, when it comes to data protection, it is always more profitable to take pessimistic approach with much caution. According to the report of the American Small Business Association (SBA) more than 99% of all firms that have employees are small enterprises. Doing so, they employ 50% of all private sector workers and provide nearly 45% of the salaries of the population. In the EU, SMEs account for 99.8% of over 19 million companies, employ 66% of the working population, and generate 54% of total turnover*[5]*. However, SMEs are the most vulnerable in a crisis just because they are small.

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*[6]*. In the light of recent experiences related to natural disasters and the situations that occurred after them, SBA emphasizes that only those firms that were well prepared for emergencies had returned to work.

In the analysis of business, small companies should always ask themselves the following*[7]*:

- Is the SME prepared to relocate temporarily?
- Does the SME have copies of, and access to, vital business records? (The SBA recommends backup data is stored at an offsite location at least 80 km away from the head office.)
- Does the SME have access to vital business applications? (emergency payroll, accounting, access to suppliers and resources)
- How much data would the SME lose in a disaster between backups?
- How quickly can the SME recover from a disaster?
- How long would the SME be without a connection to its customers?

An example of a potential crisis situation

The reasons and the moments of occurrence of crisis situations are very diverse, and, also, scenarios under which the crisis appear. One, of many possible emergencies, could follow the following scenario:

- At the end of the D-Day, around 3PM, the main and only server in the agency that deals with record-keeping for several SME, the server suddenly crashes due to an unknown reason. Employees try to restart the computer to return server back to work. After unsuccessful attempts, because SME has no contract for the permanent maintenance of equipment, they call reseller, which should fix the system. Soon, it

comes the end of working time and none from the reseller company is able to repair the server. Clerk writes down the symptoms and promises that repairer will come the next day to SME to fix the system. The last backup was made and saved on the day D-1 at 11PM. Data from the D-Day have remained unrecorded in the server.

- In a rather optimistic case of the solution of the problem, repairer comes to the agency in the morning of the D+1 day and starts to test the system. Testing determines that the error is in the hard disk and that there is only one hard drive in the computer. He installs a new hard drive, installs the OS and user programs from the installation discs and the last usable backup data transfers to the hard drive. After repairer tested the server, and lifted it up and connected to the network, he restarts the network and makes the network ready to work. Repairer ends his job at 5 PM. Now, there are in the server the data which were last updated on the day D-1 at 11 PM. Data from the D-Day have been lost. Because the employees could work on their work stations some jobs in "off-line" mode, data from the day D+1 are partially stored into the workstations, but not the server. An employee remains in the company over time to transfer data from workstations to the server for the D-Day and the day D+1.
- On the day D+2 server is ready to work. Employees begin to reconstruct the data that were not preserved and were not entered into the database last night. Reconstruction ends before the end of working day and the system is fully operational.

This is, almost, an ideal case of server repair in the case of failure of the only hard drive. The ideal is that the repairer is at the same time repairer of both, hardware and software, that he has had the necessary hardware and software, that the backup was done and preserved in good condition, that a part of the data was stored in the workstation and was ready to be transferred to the server. In this situation, firm lost practically three days because of server.

Any other scenario is much worse. It is possible that the repairer has no corresponding parts and need to procure them from the manufacturer, or, the backup is with failures and it is needed to take some older backup, or, there are no employee who can work overtime to make data entry in the server, or, workstation does not store data that are intended for the server, or ... In any of such situations the system could be repaired much later, and the costs would be significantly increased. It goes without saying that server's crash also affects the performances of the companies whose records the agency keeps.

Therefore, for each SME, it is very important to look at what can be done to minimize the risk of such crises.

2. MEASURES TO BE TAKEN BY SME IN DATA PROTECTION

Although the first thought of the SME leadership is the selection of appropriate technology, the first step should always be the selection of the right people, policies and procedures. Procurement of equipment should be realized only when there are clearly defined the needs of the system. This could save up part of the funds, because prices of IT equipment are constantly falling. In SMEs, it is unlikely that there is a special service for IT and data protection. It is much more frequently the case that SME designates an employee of the Company, as the person responsible for data protection. That person is responsible for research of the protection measures, software and hardware buying, system testing and user training. It has the obligation to document the process, because any eventual absence of that person could lead to high risk for the system.

The person responsible for data protection, at the very beginning of his/her 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. In medium-sized enterprises, that group can be composed of, for example, directors or heads of individual services or departments. In small companies, rather than groups, often it is enough that the person responsible for the protection consults company owner, or its executive director. The responsible person must be familiar with relevant laws and regulations that affect or may affect the priorities of protection.

On the basis of requests of business' technology and users' needs, the person responsible for data protection, in collaboration with the company's management, defines the field of protection. Most SMEs are usually focused on the protection of one or two applications, primarily due to limited resources. That way, good results could be achieved with limited resources.

In order to predict required investment in the protection, it is necessary to estimate the losses caused by a single failure of the system. This is very problematic for a small company that just enters to the business because new company does not have adequate data. In such cases, when there exists no personal experience, as a landmark can serve the experiences of similar small businesses. Approximate cost of a single failure can be obtained from the following formula:

$$Co_1=(\Delta\tau_o + \Delta\tau) \cdot (n \cdot HR + LR)$$

where:

Co_1= cost per occurrence

$\Delta\tau_o$ = time of outage

$\Delta\tau$ = time between two consecutive backups

n = number of employees affected by the system fall

HR= average hourly wage of the employee affected by the system

fall; This value, with satisfactory accuracy, can be obtained if the total monthly wage of employees, in that part of the middle-sized enterprise, is divided by the total number of working hours. In small companies, with sufficient accuracy, the total monthly salaries of all employees can be divided by the total number of working hours of all employees.

LR= lost revenue per hour. It can be calculated in different ways, but a good enough indicator could be the profit per hour recorded in the same month in previous calendar year multiplied by the coefficient of growth achieved in the current fiscal year compared to same period the previous year.

The size of investments needed in data protection can significantly affect the desired recovery time of the application (DRA) and the allowed time of data loss (ADL). DRA refers to the required time in which applications should be capable of working again, and ADL refers to the time that will be acceptable short not to lose much of the data entered. If that times are shorter, one can expect higher costs.

The results, achieved by the assessment of costs, have to be presented to the company's management, and the management will decide about the acceptance or non-acceptance of proposed measures and investments.

It is extremely important that one copy of the data, also, are stored on another location. The reasons are numerous, including the possibility of fires, floods, earthquakes, theft, etc.. The cheapest alternative is when the data are stored on a secure location that is hundreds of kilometers away from the server's location. That way, one can avoid risk of all natural disasters, fire and theft. However, the problem of data protection appears at the remote location. One possibility is to store data on servers of the Internet service provider, or in the premises of the network administrator, if the network administrator is doing his job remotely.

3. SELECTION OF DATA STORAGE TECHNOLOGY

When the DRA and ADL are defined, and when the budget is defined, then 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 (eg mode of business operation: one or more locations), appropriate technology should be chosen very carefully.

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:

- **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.

Compared to solutions with synchronous replication, this approach offers a lower server load, faster update and corrections, and the possibility that the replication is done through the Internet network with low bandwidth. Software-based replication solutions can ensure the recovery of servers and applications with excellent DRA, so users can continue to work just minutes after the crash.

Given that today's hardware costs are not high, all the current servers, due to security reasons, should provide the opportunity to work at least in RAID 1 mode. According to this standard data are recorded on multiple (at least 2) identical disks. Disk array provides safe operation in case of relegation, or crash of a hard disk, and the system is functioning normally as long as there is at least one correct hard drive. In this way it avoids a crash of the system due to failure of one hard drive, but it does not solve the problem for the need to store data on an off-site, away from the main server. Because of differences in labeling, that was appeared at the various manufacturers of computer equipment, a new division of RAID systems was introduced. Under the current division, data protection system designers have at their disposal:

- Failure-resistant disk systems – FRDS
- Failure-tolerant disk systems – FTDS
- Disaster-tolerant disk systems – DTDS

For sure, the DTDs are fastest and most desirable solutions to use, because they allow to operate freely in virtually all circumstances, but they are also the most expensive. Therefore they are used mainly in the applications where the importance of applications is exceptional, and, consequently, the high cost of investment is acceptable.

4. HOW TO SIMPLIFY DATA PROTECTION?

It is obvious that many SMEs do not have enough qualified staff that could respond immediately to every crisis situation. Many SMEs engage for these jobs associates or agencies, on the principle of a monthly engagement or engagement when required. Therefore, it is convenient, besides the use of FRDS, FTDS or DTDS solutions, to have automated operations that are carried out regularly in order to protect data. In this area, of a great help are software developers.

Today's operating systems, especially server operating systems, have the ability to record the current situation, either in predefined time intervals, or at the special request of the user, for example before installing of the new software. This allows users that easily bring the system to a previous working state after a crash. Normally, changes made after the last recorded valid snapshot are lost. Theoretically, the intervals between the two snapshots of hard drives might be short, but given that the snapshotting hard drives takes a lot of time, this activity should not be run too often, because it slows down the use of computer. When some unwanted changes to documents have occurred, users can simply call the last correct image of the hard drive to select the desired file, to review his versions and to choose the desired version. It is fortunate that an application software also makes its own backups, so that in the event of an unplanned and unwanted software crash much of the data can be recovered.

This approach eliminates another part of the potential problems in data protection, but not all the remaining problems.

5. CLOUD-STRATEGY AS A POSSIBLE SOLUTION FOR SME

"Cloud computing" is a general term for anything that involves the delivery of hosted services over the Internet. These services can generally be divided into four groups*[9]*:

- Software-as-a-Service (***SaaS***)
- Infrastructure-as-a-Service (***IaaS***)
- Platform-as-a-Service (***PaaS***)
- Desktop-as-a-Service ***(DaaS)***.

The point of the idea is that computing is not performed on the user's computer, but in the cloud (somewhere on the Internet). Cloud-computing presents solutions that can work anywhere, at any time and from any device, without need that the software have to be installed on the user's computer, for example, on PC or notebook. This concept is now available, because there are relatively good connections between users' computers and the Internet.

This strategy can be a cost effective solution for SMEs. It is enough that the SME has simple PC computers connected to the Internet, and to conduct its operations with the help of service provider that can be located anywhere in the

world. Assuming that the SME chose good service providers, the successful operation requires only a secure the Internet connection. Computer located in the premises of the SME can be any "thin" client. The Internet, or, more precisely, service providers act as a server. Since this is a relatively new strategy, many small and medium enterprises are still not decided on the transfer of critical applications and data into the cloud.

One of the arguments against the cloud strategy is the assumption that the Internet may be not available at some point, so and databases and applications will not be available. In addition, the high costs of setting up the software and databases in the cloud contribute to the fact that companies do not use cloud services. In contrast, protection of data and applications represents a major stimulus for small and medium enterprises to use the cloud. Miroring data and applications across cloud's platforms, and a high level of redundancy of services that the cloud offers, they are one of the key recommendations for the data protection in the cloud. Cloud can be very effective solution to protect critical data and applications, because it meets almost all the conditions for their safe keeping. In addition to data protection, SMEs can feel cloud platforms also as a broader level of support, including the possibility of relocation, management and monitoring of cloud-based IT assets.

Cloud-supported data protection solutions provide a guarantee that companies can survive even if their physical IT infrastructure suffered significant damage, and/or if they are out of business for a longer period of time. The possession of such a guarantee is essential given the possible consequences of inadequate protection of IT assets. According to estimates of Contingency Planning, Strategic Research Corp. and DTI/Price Waterhouse Coopers, 70 percent of small companies that experience major data loss are disappearing from the business during the year*[10]*.

This concept is already affordable to SMEs. Services can be purchased or on the basis of membership fees (fixed fee) or by consumption of engaged resources (such as payment of electricity bills). But, according to Verizon there are many firms which don't actually have the resources for maintaining IT infrastructure and still other who don't have any dearth of resources and yet don't want to undertake the responsibility of handling the job *[11]*.

6. CONCLUSION

New business factors require monitoring and analysis of huge amounts of data. Due to the more comprehensive analyses, and fierce competition on the market, a growing number of different data becomes critical. Some data are essential in everyday activities, and they demand to be kept and to be always available. Some of the data are confidential, and therefore require a special protection. Part of the data should be available to public for advertising and other purposes and

as such should be accessible to everyone in an unchanged form. Such contents also require protection, but from another point of view. Due to the variety of demands, the protection itself varies from situation to situation. SMEs are in a special position because they have less resources and fewer personnel. Therefore they must pay particular attention to the problem of data protection. These activities should be conducted carefully and successively, in order to reduce costs and to reduce errors to an acceptable minimum.

After detailed analysis of the business technology of SMEs, potential crisis situations, possible concepts and technical solutions, before a procurement of equipment it is necessary to re-examine whether all the factors are considered and taken into account. Particular attention should be given to answering the question: Is it possible and how fast it is possible to recover system, and applications and data make available to users? It is needed to check if there is access to all parts of the system, all components that are potential sources of crisis, and whether they can be fixed quickly. Also, an important task is to establish an algorithm by which the server after a crash will be recovered. Also, because of continuing changes in business, the possibility of eventual expansion of the system, changes in individual components and increase in the number of users should always be kept in mind.

Finally, the cloud-concept should not be forgotten. It is relatively little used at present, but it is expected that in the next ten years the cloud-concept will appear as a standard solution for small and medium-sized enterprises.

7. REFERENCES

1. Žarković Z, Mala i srednja preduzeća – Halo, pomoć!, Available on March 14th, 2011 at:

   www.emins.org/sr/publikacije/evropa-plus/arhiva/serija1/broj33/5halo.htm

2. Vasić M, Kuda idu mala i srednja preduzeća?, Available on Mar. 14th, 2011 at: www.blic.rs/Vesti/Ekonomija/180515/Kuda-idu-mala-i-srednja-preduzeca

3. docuVision, Electronic Document Regulatory Compliance – Executive Overview, Available on Mar. 14th, 2011 at: www.docuvision.com/electronic-document-complience/electronic-document-complience.cfm

4. McDermott, Adian. „A Small Business Approach to Computer Downtime“, www.user_groups.net

5. Clement K, Hansen M, Environmental Incentives for Nordic SMEs, Stockholm: Nordregio 2002, ISSN 1403-2503, ISBN 91-89332-28-8

6. Cornwall J, The Enterpreneurial Mind – Recently in Learning from Failure Category, Belmont University, June 22, 2010, Available on Mar. 14th, 2011 at:

http://www.drjeffcornwall.com/learning-from-failure/

7. Double-Take Software, Inc. - Whitepaper: Six Data Protection Tips for SMBs, Available on Mar. 15th, 2011 at: ttp://hosteddocs.ittoolbox.com/six_data_protection_tips_for_smbs_wp.PDF
8. MDR Midwest Data Recovery Inc., RAID Systems: A Description and Analysis of Common RAID Types and Their Functions, Available on Mar. 15th, 2011 at: http://www.midwestdatarecovery.com/raid-system-introduction.html
9. Akka D, Do you SaaS, PasS, IaaS or DaaS?, Available on Mar.18th, 2011 at: http://web.magicsoftware.com/davidakka/bid/21575/Do-you-SaaS-PaaS-IaaS-or-DaaS
10. Kaskade J, SIOS Technology: A Cloud Strategy for SMB Data Protection, Virtual-Strategy Magazine, Available at: www.virtual-strategy.com/Features/20100602-SteelEye.html
11. Verizon introduces Cloud Computing 'CaaS' For SMB, Available on Mar. 14th, 2011 at: www.usanewsweek.com/news/Verizon-introduces-Cloud-Computing- CaaS-For--SMB-1284495955