METHODS AND INSTRUMENTS FOR ENHANCING CLOUD COMPUTING SECURITY IN SMALL AND MEDIUM SIZED ENTERPRISES

Assist. Prof. Angelin Lalev

Abstract: The article focuses on the problems of information security in the clouds from the point of view of small and medium-sized enterprises (SMEs) and the limitations imposed on them with regard to information technologies. The article discusses organizational and technical protection measures that are relatively easy and cheap enough to be applied by SMEs in relation to cloud security threats.

Keywords*:* information security, small and medium sized enterprises, cloud computing.

JEL: C88, C89.

With regard to information security, both in principle and in particular for cloud computing, SMEs represent a special group of organizations. They are extremely heterogeneous in nature, which also reflects in the drastically different information security needs each SME has. However, two important characteristic features distinguish the vast majority of SMEs from many other categories of business and non-profit organizations. **Firstly**, SMEs usually have very limited IT budgets. **Secondly**, SMEs rarely have enough personnel specialized in the field of information security.

These two constraints impede the achievement of adequate information security and make SMEs a convenient target for attacks. This is substantiated by observations in practice, where over the last 5 years we have witnessed mass attacks targeted specifically at SMEs, and especially at their e-shops. These attacks typically involve thousands of SMEs (in some cases – hundreds of thousands of SMEs) with the purpose of gaining access to bank and card data, aiming at direct theft of funds *(Constantin, 2016), (Bad bytes Security Blog, 2011)*.

One aspect of information security for SMEs, mostly affected by these limitations, refers to cloud computing. It is attractive to SMEs due to the significant cost saving as a result of transferring data processing to cloud providers. Incorporating them, however, changes the information environment in which organizations operate. This process may pose new problems and challenges to the information security of SMEs.

The article aims at formulating measures to enhance cloud computing security in SMEs. These measures are grouped in two fields – organizational and technical. Organizational measures refer to activities such as identifying data at risk and formulating organizations' data handling rules. Technical measures refer to settings and configuration of the software and hardware of information systems.

1. Threats to cloud computing in SMEs

The formulation of information protection measures and risk analysis cannot be adequately carried out if it is not based on good understanding of existing threats regarding information security in the cloud. The problem of identifying threats specific to cloud computing is related to a number of conventions.

A very important fact to be considered when formulating the different categories of cloud computing threats is that in fact, the very concept of 'cloud computing' refers to a rather heterogeneous

range of services. The various types of cloud services are exposed to a different set of threats. However, a more significant difference between them is that different service models assign different responsibilities for providing information security between organizations and cloud providers. That is, in certain service models, cloud providers are responsible for threats, while in other models, threats are the responsibility of organizations.

There is an inverse relationship between the flexibility of cloud services and the amount of information security activities delegated to cloud providers. IaaS services offer the greatest flexibility and enjoy the most popularity, but they delegate information security activities to providers to the least extent. (See Table 1):

Table 1.
Responsibilities of cloud service customers with regard to major repetitive activities intended to provide information security

	Cloud security update	**Application software update**	**Network services configuration**	**Firewall configuration**
SaaS[1]	No	No	No	No
PaaS[2]	No	Yes	Partial	No
IaaS[3]	Yes	Yes	Yes	Yes

The approximate relationship between the activities described in Table 1 and the possible threats addressed by these activities are presented in Table 2. The two tables show that the choice of PaaS or IaaS services still requires enterprises to implement technical measures to deal with very serious potential security threats, while SaaS services are more likely to require organizational measures.

[1] 'Software as a Service'.
[2] 'Platform as a Service'.
[3] 'Infrastructure as a Service'.

Table 2.
Threats to information security addressed by the activities presented in Table 1

Activity/Measure	Most common threats related to improper or incomplete implementation of the activity/ measure	Effect	Risk
Cloud security update	Viruses, worms, 'exploits', theft and change of information.	Establishing complete control over the attacked servers.	Direct theft of funds. Issuing documents with fake content. Theft of personal data. Impossibility to easily detect the source of the breach. Long downtime when troubleshooting.
Application software update	Viruses, worms, 'exploits', theft and change of information. Prerequisites for attacking the operational system.	Establishing partial control over the attacked servers.	Direct theft of funds. Issuing documents with fake content. Theft of personal data.
Network services configuration	Theft and change of information.	Prerequisites for attacking application software.	Theft of personal data. Direct theft of funds.
Firewall configuration		Prerequisites for attacking network services.	Downtime, indirect effects.

In addition to the above-mentioned threats, which can be defined as 'universal' and which affect almost any computer system connected to the network, the cloud environment offers unique security challenges that need to be addressed. Some of the most important are as follows:

- the use of cloud services involves new participants in security activities. These are the cloud providers, whose negligence, attitude and goodwill become a crucial security factor, since cloud providers have, perforce, full access to organizations' data in the cloud. For this reason, delegating data processing raises not only technical but also legal issues.

An important case in this regard is the invalidation of the US-EU Safe Harbor Act by the European Court of Justice in 2015. This agreement governed the jurisdiction over the data of EU companies when it is physically located on servers situated in the United States. The Act was repealed by the court on the grounds that it does not offer adequate legal protection for the personal data of EU citizens. Its invalidation demonstrates that the failure to adequately protect data against malicious activities by cloud providers may result in banning the transfer of certain categories of data (such as personal data) to the clouds *(Meyer, 2016)*.

For SMEs, similar prospects transform into risk, since such developments have the capacity to seriously affect SMEs' information infrastructure and their presence on the Internet, provided that SMEs use cloud computing in their activities.

- cloud services perforce 'open' organizations' IT infrastructure to the Internet, eliminating some of the usefulness of the firewalls and making infrastructure security much more dependent on cryptographic measures. The implementation of cryptographic measures is never a trivial task due to the constant evolution of this matter, which in principle requires very serious knowledge and skills for proper implementation.
- cloud services (especially public SaaS services such as Gmail, Drive, etc.) provoke the use of information from home computers and mobile devices, which may be particularly negative for the security of sensitive information.

The features described above suggest where risk assessment as well as the follow-up protection measures should be addressed to in SMEs. However, each enterprise should

individually estimate the impact of the threats described on the information environment in which the enterprise operates.

2. Risk assessment in SMEs

As already mentioned, the problems with SMEs in determining what data needs additional protection are inherently methodological. Most enterprises in this category do not have the necessary knowledge, time and resources to conduct detailed analyses. In addition, such enterprises rarely have experience with measuring and quantifying risks of any type. Therefore, it would be extremely useful for them to formulate a set of methods that are easy to implement in a similar environment. Among the many risk assessment methods, two can be distinguished that meet the above requirements.

Business impact analysis is a common method suitable for application by organizations with relatively low culture and knowledge in the field of information security. Its principles are defined in ISO 22301 and ISO 22313. The method is used to formally assess the damage caused by business interruption.

Business impact analysis has many varieties but is always based on identifying critical business activities for enterprises and determining the maximum periods for which these activities may be interrupted. The analysis includes a series of steps *(Wrenn, 2011),* some of which are the following:

- preparing or obtaining detailed descriptions of information systems in organizations;
- determining the critical business activities by analysing the interdependencies between them;
- defining the relationship between information systems and critical activities by identifying key stakeholders (inside and outside organizations);
- identifying the worst possible times when information systems in organizations may be interrupted;

- determining the resources needed for the critical processes, including those related to the information processing (e.g. staff, network access, etc.);
- defining the so-called 'Recovery Time Objective' or 'RTO' – the time needed to restore the activity of critical business systems;
- determining the maximum allowable time for which information may not be available **after the information systems are restored and resumed** – 'Recovery Point Objective' or 'RPO'.

Applied to cloud computing, these steps make it easier to identify information that is critical to organizations and is potentially exposed to cloud risks.

Business impact analysis has several fundamental weaknesses:

According to the standards, business impact analysis is designed as a comprehensive procedure to assess enterprises' preparedness to deal with disasters and accidents of all kinds – i.e. many of the prescribed steps and principles in the process of conducting it are not directly related to information systems in organizations and are even less related to the use of cloud computing;

Another more serious drawback is that **business impact analysis is specifically oriented to the damage caused by *interrupting* enterprise activity and, in the case of cloud computing, the operation of information systems**. Apart from interruption, however, disruptions in information security of organizations usually lead to other effects outlined by the classic 'CIA triad' (*Schwartau, 2001*). **According to the CIA triad, business impact analysis focuses only on the effects of data breach. However, another thing should also be considered, namely that violating the other two aspects – confidentiality and credibility, together with interrupting the activity for conducting audit, reinstalling, and recovering data from archives can also lead to much more severe consequences and losses.**

Some other weaknesses are as follows:

- direct theft of funds from bank accounts of companies;
- customer disappointment and a possibility of losing them;
- fines imposed by regulatory bodies;
- opportunity costs and competitive advantages, including concluded contracts and attracted consumers.

The amount of damage is not directly related to the way business processes are organized and depend on each other, and the business impact analysis approach can hardly bring any useful information for their assessment.

The fault tree analysis method provides the basis for both qualitative and quantitative analysis. In addition, the method focuses on determining the probability of occurrence of a scenario that complements the above-mentioned business impact analysis method. A variation of this method, developed in the 1990s (*Salter, 1998*), is known as the 'attack tree'.

According to the authors of the method, each attack against the security of an information system includes three stages – identifying a weakness, gaining access, and performing the attack. A system can be qualified as 'weak' if it does not provide sufficient measures against the implementation of the three stages of the attack.

The attack tree is an oriented tree. The top level /the root node of the tree/ represents the effect of the materialization of attacks. This may be, for example, theft of information about a company's clients, or for example theft of funds from a company's bank account.

The second level sets the life cycle stages of information systems, such as design, development, introduction, decommissioning.

At the lower levels, threats to information security at each level of a system's life cycle are deductively systematized. For each

top of the tree, all known possible ways to materialize the described threat are listed. For instance, theft of data on a company's clients may be due to a remote theft from information systems, disclosure by an insider, etc. In turn, a theft from information systems may be as a result of social engineering[4] or a consequence of hacking attacks.

The individual nodes in the tree represent links of the type 'AND' / 'OR' manifesting how combinations of factors can cause the materialization of a threat. The shaped tree allows a simple analysis to be carried out – a threat is selected and tracing the nodes in the tree shows which factors can lead to the possible materialization of the threat. Probabilities can be added to each tree top to allow the total probability of an event to be calculated.

The main advantage of the method is that it clearly presents the relationships between the different factors and threats, which is a great basis for a qualitative analysis. A disadvantage of the method is that the calculation of exact probabilities depends on the correct measurement of the probabilities of materialization of each factor or threat. The latter is labour-consuming and can only be carried out approximately, which, with the accumulation of the number of factors, would cause drastic deviations in the ultimate probability.

Both methods are only part of a relatively large set of methods and approaches for qualitative and quantitative risk assessment. In the presence of time and desire, SMEs can combine more than 20 methods, described in ISO 31000, when conducting their analyses. However, it can be concluded that the analyses carried out by SMEs will be more inaccurate and more approximate than the ones done by larger organizations regardless of the methods chosen.

[4] Fraud where the attacker aims at manipulating the people working with an information system, not at circumventing technical protection measures.

3. Measures to protect SMEs' information in a cloud environment

In view of the circumstances presented, it is quite logical to bring forward the question whether there are measures enhancing the resilience of cloud computing against various potential threats while not producing substantial recurrent costs and which are principally cheap enough to avoid the necessity their use to be the subject of precise cost-benefit analyses. The answer is in many cases positive, on condition that many of these measures reduce the risk, but to levels that remain far from those considered 'maximum' reliable. Such measures can be divided into technical and organizational, as clouds eliminate the responsibility of the enterprise for the physical aspect of information security.

The following **technical measures** stand out as particularly effective and at the same time cheap and easy to implement.

1) upgrading browsers to the latest update

Over 99 percent of the Internet users use one of the five major browsers – Chrome, Edge, Mozilla Firefox, Safari, and Opera. Years of practice so far has shown that only these five major software projects for browser development are able to simultaneously maintain the constantly changing standards for web technologies and quickly correct detected errors. If an enterprise uses another mobile or landline software as a browser, efforts should be directed towards replacing it with one of the browsers mentioned. Upgrading mobile browsers is a particular challenge in this direction. Very often it cannot be done effectively for old mobile phones and tablets, which makes it necessary to replace them or to develop an access policy that excludes such devices.

2) prohibiting the use of outdated cryptographic protocols by browsers and servers

Most browsers have additional security settings and a set of ciphers used by a browser. The standard set of ciphers is a compromise between the ability to access most Internet sites and security needs. Enhancing security by turning off old cipher sets will

'break' the access to many sites on the Internet, but not to the typical SaaS, PaaS and IaaS advanced services. This can be compensated for by introducing the use of two browsers in SMEs – a 'standard' and one that is intended to access company data and cloud applications.

3) activating security measures against exploiting software and operating system errors

Operating systems have additional security mechanisms that prevent attacks against client and server software as well as against the very operating system. They are as follows:

- Data execution prevention;
- Protection against null pointer dereference;
- Address space layout randomization;
- Detecting and preventing Heap Spray attacks;
- Structured exceptions handling;

The listed techniques can be activated relatively easy either directly or through widely available utilities. This activity can be done by both servers and customers. However, the implementation of these measures may prevent the operation of the application programmes, as in rare cases the behaviour to which measures are directed to is part of the normal operation of a fully legitimate programme. A matter of testing is to determine whether any programmes exist that are not compatible with a given measure.

4) enabling HTTP Strict Transport Security (HSTS) on cloud company servers

Enabling HSTS allows protection against a particular class of fundamental attacks which completely remove cryptographic protection from the connection between the server and the client. The proper implementation of HSTS requires that SMEs commit themselves to paying the necessary costs for electronic certificates and maintaining the necessary infrastructure in the long run, since once activated, this measure remains effective for at least a year.

5) enabling mandatory access control by servers

Mandatory access control, unlike discretionary access control, allows administrators to set security rules that cannot be

disabled by the user. This feature is used to create unique, precise profiles for each application that determine the resources the app can have access to.

A number of **organizational measures** are also very important for SMEs. Implementing them in SMEs is actually easier than in large organizations, and generally involves measures to prevent sensitive information from being placed in the clouds first.

1) **Using the Traffic Light Protocol (TLP)**. The TLP defines four levels of privacy (*USCERT, 2017*). They are as follows:

- Red – information labelled 'Red' should not be shared with anyone except the people from whom it comes.
- Yellow – information labelled 'Yellow' can only be shared with a limited number of employees within an organization whose duties are directly related to it.
- Green – information that can be shared with all the employees within an organization. However, it cannot be shared outside organizations.
- White – information that can be freely shared inside and outside organizations.

In terms of the clouds, the Traffic Light protocol is an extremely convenient means of labelling information, since the selected privacy levels correspond to the problems of sharing 'sovereignty' over data. For example, 'red' and 'yellow' levels definitely imply storing information physically within an organization, while the information labelled 'white' is publicly available, i.e. it is not a source of storage and processing problems in the public cloud environment.

The Traffic Light protocol is designed to be simple and easy to understand and use. Moreover, TLP is not bound by technical means of realization and can be applied to both electronic and paper documents. Therefore, these are its main advantages.

The main drawback is that the TLP is not in any way bound by electronic means of realization and the compliance with the restrictions is entirely the responsibility of the users. Another important weakness of the TLP is that it can be applied much more

easily to unstructured documents than to structured information and databases.

2) **Using virtual data rooms**. Virtual data rooms are named by analogy with real corporate repositories of documents where documents are sometimes only used in data rooms without their physical removal from repositories. The products offered as virtual data rooms also aim at electronic documents. They limit the user-accessible functionality of reading a document by attempting to prohibit recording, forwarding, printing, and other activities related to documents that could be used to steal their contents.

Virtual data rooms have a number of advantages over the TLP, the main of which is that, due to the approach chosen, access to documents is regulated centrally and automatically. For cloud computing, this means that virtual data rooms can prevent accidental transfer of sensitive information to the cloud.

In turn, virtual data rooms have many disadvantages. They offer security based on hiding and cannot stop a well-motivated attacker having the knowledge needed. Such an attacker may possibly create a software that circumvents protection and can multiply it across a wide range of users. Therefore, the security guaranteed by virtual data rooms can be completely lost at any time.

3) **Using Enterprise Digital Rights Management** (eDRM) or sometimes **'Information Rights Management'** (IRM) solutions. These solutions include cryptographic document security, which is checked at each opening. They are similar in design to virtual data rooms, but are much safer, since cryptographic protection means that circumventing them is much more difficult. The most successful solutions are incorporated in Microsoft Office, and although they require paid components, medium-sized enterprises can afford to incorporate them.

*
* *

The protection measures examined demonstrate that the availability of sufficient information is a more important factor than the available information security resources. The availability of multiple open source solutions and the fact that the software used has enough functions to precisely set up security measures is a positive circumstance for SMEs and shows that methodological guidance has the potential to enhance the security of SMEs.

The development and dissemination of methodological guidance on information security will be strongly promoted if there are agencies and programmes specifically involved in this activity. Such agencies operate in the United States and the United Kingdom. Unfortunately, similar agencies in Bulgaria are still developing their activities.

The implementation of such measures and methodologies is also useful for SMEs less exposed to risk, since the accumulation of knowledge and the transformation of company culture takes time. With the growth of enterprises and the use of cloud services, inappropriate implementation of such transformation can become a major factor in undermining information security and can lead to catastrophic direct losses.

References

Bad bytes Security Blog. (14 Sep 2011). Downloaded from http://bad-bytes.blogspot.bg/2011/09/revisting-recent-oscommerce-mass.html

Bozhikov, A. (2014). Oblachnite uslugi i vazstanovyavane ot IT bedstviya i avarii. *International Scientific Conference „Information Technologies in Business and Education“, UE-Varna.*

Constantin, L. (13 Oct 2016). *Thousands of online stores compromised by credit-card theft*. Downloaded from PC World: http://www.pcworld.com/article/3131040/security/thousands-of-online-shops-compromised-for-credit-card-theft.html

ISO 22301. (2012). *Business continuity management systems - Requirements*. Downloaded from https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en

ISO 22313. (2014). *Societal security — Business continuity management systems — Guidance*. Downloaded from https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-1:v1:en

ISO 31000. (2009). *Risk management.* http://www.iso.org/iso/home/standards/iso31000.htm.

Meyer, D. (Feb 2016). *Fortune Magazine*. Downloaded from Here comes the Post-Safe Harbour EU Privacy Crackdown: http://fortune.com/2016/02/25/safe-harbor-crackdown/

Radeschütz, S., Niedermann, F., & Bischoff, W. (2010). BIAEditor:matching process and operational data for a business impact analysis. *Proceedings of the 13th International Conference on Extending Database Technology, EDBT '10.*

Salter, C. (1998). Towards A Secure Systems Engineering Methodology. *New security paradigms (NSPW'98)*, (pp. 2-10).

Schwartau, W. (Aug 2001). Network Security It's About Time: An Offer for a Metric. *2001*(8), 11-13.

Tjoa, S., Jakoubi, S., & Quirchmayr, G. (2008). Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology. *Third International Conference on Availability, Reliability and Security. ARES 08.*

USCERT. (16 03 2017). *Traffic Light Protocol Matrix and Frequently Asked Questions*. Downloaded on 16 03 2017 from https://www.us-cert.gov/tlp

Wrenn, G. (2011). *Ten steps to a successful business impact analysis.* Downloaded from TechTarget: http://searchsecurity.techtarget.com/tip/Ten-steps-to-a-successful-business-impact-analysis

BUSINESS management

D. A. Tsenov Academy
of Economics, Svishtov

Year XXVII * Book 2, 2017

CONTENTS

Submitted for publishinq on 13.06.2017, published on 22.06.2017,
format 70x100/16, total print 50

ISSN 0861 - 6604

BUSINESS management

BUSINESS management 2/2017

PUBLISHED BY
D. A. TSENOV ACADEMY
OF ECONOMICS - SVISHTOV

2/2017

TO THE READERS AND AUTHORS OF "BUSINESS MANAGEMENT"

The journal of "Business Management" publishes research articles, methodological articles and studies, review articles, book reviews, commentaries and good practices reports.

1. Volume:

- Articles: between 12 – 20 pages;
- Other publications (review articles; book reviews, etc.): between 5 – 10 pages.

2. Submission of materials:

- On paper and electronically at one of the following e-mail addresses: bm@uni-svishtov.bg or zh.tananeeva@uni-svishtov.bg

3. Technical requirements (the article template is can be downloaded from the webpage of the journal):

- Format – Word for Windows 2003 (at least);
- Font – Times New Roman, size 14 pt, line spacing 1,5 lines;
- Page size – A4, 29–31 lines and 60–65 characters per line;
- Line spacing 1,5 lines (at least 22 pt);
- Margins – Top – 2.54 cm; Bottom – 2.54 cm; Left – 3.17 cm; Right – 3.17 cm;
- Page numbers – bottom right;
- Footnotes – size 10 pt;

4. Layout:

- - Title of article title; name, scientific degree and scientific title of author – font: Times New Roman, 14 pt, capital letters, Bold – centered;
- - Employer and address of place of employment; contact telephone(s) and e-mail – Times new Roman, 14 pt, capital letters, Bold – centered.
- - Abstract – up to 30 lines; Key words – from three to five;
- - **JEL** classification code for papers in Economics (http://ideas.repec.org/j/index.html);
- - Introduction – it should be from half a page to a page long. It should state the main ideas and/or objectives of the study and justify the relevance of the discussed issue.
- - The main body of the paper – it should contain discussion questions, an outline of the study and research findings/main conclusions; bibliographical citation and additional notes, explanations and comments written in the footnotes.
- - Conclusion – it should provide a summary of the main research points supported by sufficient arguments.
- - References – authors should list first references written in Cyrillic alphabet, then references written in Latin alphabet.
- - Graphs and figures – Word 2003 or Power Point; the tables, graphs and figures must be embedded in the text (to facilitate language correction and English translation); Font for numbers and inside text – Times New Roman, 12 pt;
- - Formulae must be created with Equation Editor;

5. Citation guidelines:

When citing sources, authors should observe the requirements of **APA Style**. More information can be found at: https://www.uni-svishtov.bg/default.asp?page=page&id=71#jan2017, or: http://owl.english.purdue.edu/owl/resource/560/01/

6. Contacts:

Editor in chief: tel.: (++359) 631-66-397
Co-editor in chief: tel.: (++359) 631-66-299
Proofreader: tel.: (++359) 631-66-335
E-mail: bm@uni-svishtov.bg; zh.tananeeva@uni-svishtov.bg;
Web: bm.uni-svishtov.bg
Address: "D. A. Tsenov" Academy of Economics, 2, Em. Chakarov Str., Svishtov, Bulgaria