NECESSITY OR CHALLENGE - INFORMATION SECURITY FOR SMALL AND MEDIUM ENTERPRISES

CSABA LÁBODI, PÁL MICHELBERGER [*]

ABSTRACT: *Due to the inadequate mamagement of information security expectations and various unexpected information technology incidents, small and medium enterprises that lose data or have to cope with a lack of data over a certain period of time may lose business commissions or customers. A solution to this problem may be the regulated administration of information security, which may lower the amount of risks. Enterprises in this sector generally have not enough human, material and information technology resources to perform tasks of this sort. The controversy seems to be an irresoluble one; the authors attempt to provide help to initiate a solution to the issue that remains above the 'still acceptable' level. The paper surveys several professional sources as well as standards, recommendations, and methodologies applicable in the field. The authors of this paper consciously strive to differentiate between information technology security and information security.*

KEY WORDS: *SME; information security; IT security; integrated management system*

JEL CLASSIFICATION: *L19, M15*

1. INTRODUCTION

It is proven by two international surveys (SMB Disaster Preparedness, 2009); (Outpacing change, 2009) that enterprises do not put adequate weight on IT security and information security. The situation is especially disappointing in the case of SME - small and medium enterprises. Their business environment and the demands they have to meet keep changing rapidly; in addition, these organisations (as a result of their size) are more flexible than large companies. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250

[*] *Private Lecturer, MSc, University of Pannonia, Faculty of Economics, Department of Applied Economics, labodi.csaba@almos.uni-pannon.hu*

Prof., Ph.D. ,Óbuda University, Keleti Károly Faculty of Business and Management, Institute of Management and Organisation, michelberger.pal@kgk.bmf.hu

persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro in EU (Slusariuc, 2004). Their information security activities (or the absence thereof) present lower risks but require constant supervision and renewal. Professional sources provide numerous ideas and proposals regarding the way to reach and maintain a higher level of information security with fewer available resources. We attempt to provide guidance to the members of the SME sector in the development of their information security activities with the help of useful ideas quoted from our sources, our own experience, and the relevant background of standards.

2. INFORMATION SECURITY AND IT SECURITY

In a society and economy increasingly based on knowledge, information is a business company asset which lies at the heart of managerial decisionmaking as well as success in business; it is at the same time the "power source" of the applied information technology, thus being a decisive factor in efficient operation. Among other things, information may be related to products, services, technology know-how, available resources, or business partners. If information is missing, inaccurate, out-of-date, or if it lands in unauthorised hands, the enterprise may face damage. Information thus needs to be protected...

Today this means (ISO/IEC 27001):

- **confidentality** (the information must be available exclusively to authorised parties);
- **integrity** (the wholeness and exactness of the information must be preserved);
- **availability** (authorised users must acces the information when necessary).

Information security is a far more complex issue than IT security. Nowadays it is not enough to think in terms of antivirus programmes, firewalls, reliable hardware and unambiguous identification systems. The conscious construction of the technological background no longer suffices. The integrity, availability, and confidentiality of information is primarily threatened by negligent handling or purposeful damage at the hands of internal employees (through company information control systems and the intranet) and strategic partners with access through the internet, extranet or Electronic Data Interchange to company databases (suppliers, retailers, cooperation partners and financial service providers). Several other qualities, such as accuracy, accountability, non-repudiation, and dependability may also be linked to information security.

Generally, it is the handling of information and information carriers that is regulated in order to protect information property. This is independent from the form the information is presented in. Protection functions well if the information to be protected is defined, along with internal and external threats, the risks posed by these, and the regulations and means of protection (ISO/IEC 27002). Threats to the company "information property" may be manyfold; the list below is far from complete: erroneous seftware applications, malfunction, unprofessional/inefficient information technology planning and operation, unauthorised use or access, natural disaster situation (fire, flood, earthquake), viruses, spy programmes, sniffing and spoofing, unpermitted software use, unqualified workforce, deliberate fraud or misuse, abuse.

The aim of information security is to ensure the continuity of business in a structured manner and mitigate damage caused by security events. Information security may be achieved with the application of protective measures, taking risks into consideration. These consist of regulations defining company processes, the company structure reflecting these processes, and the regulated operation of IT tools (hardware, software, telecommunications devices) appropriate to them.

Information security is a state. In order to ensure the long-term operation of business organisations, the application of a system providing security is necessary (instead of means and devices that give a false sense of security). Professional sources define several interconnected dimensions or levels of security. Ji-Yeu Park and co-authors speak of three further "layers" beyond the adequate handling of IT infrastructure (hardware, software and network protection) Infrastructure Level (Ji-Yeu Park, et al., 2008): *Information Level* (e.g.: who may use, add, modify or delete what data…); *Workflow Level* (process control, workflow); *Organisational Level* (individual and group decisionmaking, information security strategy, risk management). A good example to this is the "holistic" structuring of the authorisation system. All four levels have related tasks:

- IT level - user identification;
- Information Level - ensuring access only to data minimally required to perform the work;
- Workflow Level - the division of critical processes, location- and person-bound authorisation (it is frequent within SMEs to "pass on" the password and log on simultaneously with the same password from various locations…);
- Organisational Level - risk avoidance, the creation of authorisation groups and the regulation of the constant supervision of the authorisation system.

Another source also defines four elements to be examined and regulated in the case of an information security system created for SME (Hangbae Chang, et al., 2006): technical elements or Component (purchased hardware and software, network tools); knowledge and experience elements or Human IT (as the company uses IT elements…); shared information service elements within the company (for end users); shared and Standard Applications, e.g.: ERP systems (training and support for users).

The creation of a supportive environment to information security is also important, which means an accepted information security policy, clearly defined areas of responsibility, training, and the assurance of financial resources. Only after all this may information security as a state be created. Among other things, this involves the full registration of IT devices and documentation, risk assessment (for IT devices and the challenges of the environment), and the handling of user authorisations (for access to documentation, networks, servers, workstations, application software, and the information itself).

3. INFORMATION SECURITY MANAGEMENT SYSTEM

SMEs usually do not have adequate human, material, and technical resources to properly manage information security. For these organisations, it may be especially important to make transparent the related activities and tasks. A simple management method used in the English-speaking territories may help to somewhat improve the poor situation created by the lack of resources (Tawileh, et al., 2007). The required level of information security may be approached or an information security management system may be created on the basis of the so-called CATWOE problem analysis model (a series of steps);

C (Customer) - What enterprise will create an information security management system?

A (Actors) - Who will create and operate the management system?

T (Transformation process) - What is the main aim of the management system?

W (Worldview) - How will the enterprise achieve this “main” information security aim?

O (Owner) - Who is the owner of the organisation and the management system?

E (Environment) - What is the effect of environmental forces on the information security management system within the organisation?

Once we can give answers to these questions we “only” need to force the enterprise into a four-step “management circle” complete with feedback, one similar to the PDCA (Plan - Do - Check - Act) cycle: the definition of company information security targets; the identification of the necessary activities; the execution of these activities; the supervision of the information security management system.

3.1. Critical company areas

Information protection is especially important for companies that: have information at the basis of their operation, or where operation is fundamentally determined by data and information; maintain links with partners by IT means, and the maintenance of electronic contacts is a major factor in external links (e.g.: logistics organisations); are involved in receiving, processing, storing, and forwarding data of other organisations or persons (e.g.: cooperating partner, client); are involved in the implementation, development, setup, and installation of IT systems (e.g.: IT companies); perform research and development work where the produced results and value basically take the shape of information; own, create, and handle confidential and private information. Nowadays this list may be extended with one other field: companies using mobile devices and the internet to distance-access services.

3.2. Standards, recommendations, methodologies

There exist several internationally renowned and accepted documents on the regulation of IT security and information security. In this subchapter, we shall mention a few of these - the ones we deemed important. Their approaches and target areas are obviously all different but all discuss the protection of company information.

Common Criteria (henceforth abbreviated CC) traces its origins to the US but has been taken over by Canada and the European Union. It is easy to recognise from the full title of the document (Common Criteria for Information Technology Security Evaluation) that it was created for the measurement and evaluation of the security levels of IT products and systems (www.commoncriteriaportal.org). A European standard version has been available since 1999 (ISO/IEC 15408-1, -2, -3).

It clearly defines for organisations performing security audits what a system must provide and how this may be examined in a way that may be exactly repeated. For developers it ensures the clear definition of security solutions and sets the requirements the delivered product has to meet. For consumers (users) it makes it possible to clearly define their requirements regarding the security functions of products and systems and compare the different security solutions. Evaluation criteria are listed in Section 2. (security functions) and Section 3. (guarantee requirements) of the standard.

ISO/IEC 2700x is an information security management system or standard package of British origin, providing guidance to information security activities (www.iso27001security.com). Companies define security requirements and related measures on the basis of business objectives and organisational strategy. Information security (integrity, confidentiality, and availability) is treated with special emphasis. It is not linked to any sort of information technology. The standard (ISO/IEC 27001) divides company operation and the related requirements into 11 protection areas, and, within these, 39 targets and 133 protection measures. The information security management system, once it has been implemented and documented, may be accredited by an independent accreditation organisation (ISO/IEC 27002). In the standard package there appear a few supplementary sections, presented as individual standards (e.g.: implementation guidance - ISO/IEC 27003; information security risk management standard with advice on selecting appropriate risk analysis and management tools and methods - ISO/IEC 27005). Development never stops. There are plans for further standards (e.g.; guidance on information security management for sector-to-sector communications - ISO/IEC 27010; guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 as IT Service Management - ISO/IEC 27013).

The **ISO/IEC 20000-1, -2** standards on the operation of information systems is based on and harmonised with the ITIL (Information Technology Infrastructure Library) recommendation of British origin (www.itsmfi.org). The first half of the document gives a formal specification and defines the requirements for an organisation to deliver managed services of an acceptable quality for its customers, while the second part is a Code of Practice and describes the best practices for Service Management processes within the scope of ISO/IEC 20000-1.

Service management activities are linked to the currently popular PDCA model, which is employed in several standards.

Beside the management system, the issues of the planning and implementation of IT services, and the planning of new services there are five areas in total service management:

- Service Delivery Processes (service level management, service reporting, capacity management, service continuity & availability management, information security management, budgeting & accounting for IT services)
- Control Processes (configuration- and change management)
- Release Process (handling the release of documents and operation manuals, documenting the approved changes)

- Resolution Process (incident- and problem management)
- Relationship Processes (customer service, the management of business and supplier contacts)

The ISACF (Information Systems Audit and Control Foundation, IT Governance Institute, USA) has developed a recommendation entitled "**CObIT**" (Control Objectives for Information and related Technology) (www.itgi.org/cobit). Practically, this material is a management tool which helps users to understand and handle risks and advantages conected to information and information technology. This internationally approved and developed "framework" was created primarily for business enterprises and is aimed at harmonising information technology services and the operation processes of the organisation as well as facilitating the measurability of the security and management features of information technology services. CObIT is a collection of documents grouping best practices according to a set of criteria. In order to ensure the necessary information for the fulfilment of organisational (business) aims, information technology resources must be managed within a framework of connected procedures. With its use, we may bridge the gap between business risks, control requirements, and issues of technical nature. The system may be used by the upper management, the users, IT professionals, and the controllers of the information system at the same time. The real aim of COBIT is the achievement and maintenance of information technology security at a minimum risk and maximum profit.

Its structure is as follows: *Executive Summary; Framework; Control Objectives* (34 high level processes, management guidelines and maturity model + management guidelines, critical success factors, Key Goal Indicators, to define target levels of performance; and Key Performance Indicators, to measure whether an IT control process is meeting its objective) Supplements (summary overview, case studies, frequently asked questions)

The recommendation defines 34 "management" goals in connection with information technology processes, dividing them into four areas: 1. Plan and Organise; 2. Acquire and Implement; 3. Deliver and Support; 4. Monitor and Evaluate. There are 215 specific and detailed control objectives throughout the 34 high-level IT processes.

3.3. Integrated management systems

In the past decade or so the acceleration and substantial transformation of technical, economic, and information technology development has furthered the creation of a strong, international economic organisation force and a knowledge-based economy, which requires complex intellectual skills in the decisionmaking process. The most effective solution for multi-factor tasks is offered by the implementation of management systems based on TQM principles[*], the EFQM (European Foundation for Quality Management) model (figure 1) or ISO standards.

Management systems harmonise subprocesses, byprocesses and control system elements, thus ensuring that the management is able to continuously control and

[*] *The principles of TQM: customer satisfaction; process management; management by fact; continuous improvement; total participation and empowerment; strategic focus and alignment; openness to innovation and changes (Tenner, A.R & De Toro, I, J., 1993)*

regularly check the processes, tools, and resources that are the decisive elements of its activity. The simultaneous and integrated application of system standards facilitates the execution of more complex tasks. The control of main and subprocesses may be exercised simultaneously with the maintenance and development of process capability, the achievement of error-free operation, the lowering of resource use and costs, the increase of profit, and the development of the work environment. There also may present itself the demand of the efficient and homogenised treatment of an upper-management area, such as for example finances, liquidity, economic decisions, the handling of the changes in the legal environment, logistics, the application of motivation techniques, communication and marketing.

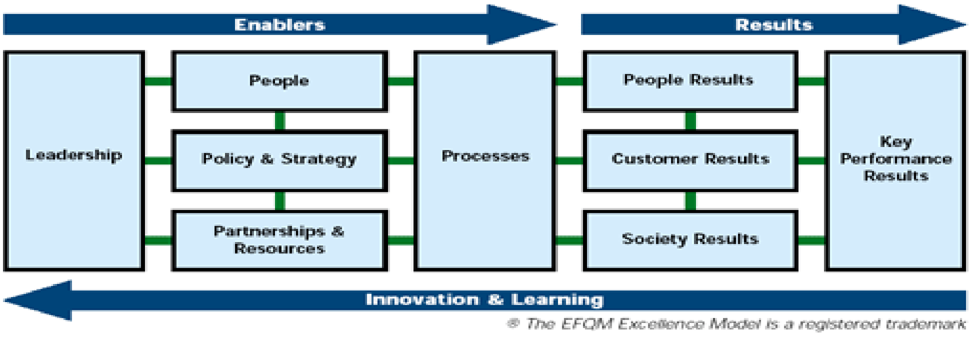

Figure 1. European Foundation for Quality Management; Excellence Model (www.efqm.org)

A sustaining element of PDCA model-based, process-centred integrated management systems is the use of information technology infrastructure. With its implementation the management of complex tasks is made simpler, more effective and more efficient; as a part of the system of value creation it contributes to the fulfilment of business expectations and the achievement of competitive advantage.

An openly mentioned aim behind the continuous reform and development of the ISO/IEC 2700x standard package is the unified treatment of divergent standard management systems (quality and environmental management systems), and the avoidance of multi-regulation for business processes. In the supplement of the ISO/IEC 27001 standard we find a table showing the connections between standards and the similarities of their structures. Many organisations have started implementing and operating so-called integrated management systems in Hungary, as well. It is probably a feasible way for smaller companies not too well provided with capital to cope with the demands of their business environment. The control, pre-audits, and accreditation of the management systems in every third year facilitates the possibility of continuous development for the organisation.

Due to the widening of on-line corporate relationships, it may be observed that smaller organisations wish to treat the control of IT systems (IT security) and the information security connected to business processes under a homogeneous regulation system.

3.4. Auditing as a possibility

Auditing is a supervisory activity executed by an independent external organisation authorised for the activity. According to the regulations of various standards, auditing may cover the main and subprocesses of the organisation, the environmental protection aspects of the activity pursued by the organisation, the related labour safety issues, the fulfilment of various specifications of the industry, the information security management system itself under ISO/IEC27001, or information technical products, or product families under ISO/IEC 15408.

The certificate issued by the organisation accrediting management systems is proof of the conduct of an objective examination conducted according to the internationally approved standards, and of compliance with the requirements of the internationally approved standards. In addition, the certificate issued about information technology products proves that the developer of the product assumes responsibility for the product up to a guarantee level assumed by himself. The possession of a certificate improves the reputation of the organisation and its products. A It results in lasting trust on behalf of business partners towards the company and thus lays down the fundaments of its success in business.

Auditing a management system also includes the examination of how clients' demands may be fulfilled, and surveys the guarantees provided by the system. The areas listed cover the prescriptions of the set of requirements observed during the implementation of the system, their adequate regulation and documentation: Security policy; Risk assessment and management; Business Continuity Plan; Disaster Recovery Plan; Declaration of applicability; Data protection, virus protection; Documentation and inspection of incidents and events; Security rules connected to jobs and persons, the existence of applicable laws, other (external) prescriptions and professional regulations, awareness of these and compliance with them; The existence of administrative - environmental (security guarding) - information technology regulations, knowledge and practice, their simultaneous application.

Naturally, the implementation of an audited integrated management system is not always possible due to the lack of resources but the holistic examination of the company's work may lead to "integrated" security.

4. INFORMATION SECURITY AWARENESS

Physical security and protection means the creation of the necessary environment, to fend off accidental or deliberately caused damage or disasters. The areas of logical security and the related operative protection are as follows: data protection (personal and business data); application level protection (log); access and authorisation systems; saving and archiving systems; the regulated operation of the links between the internal and the external net; software protection of IT devices (e.g.: virus control); worst-case scenarios in disaster situations.

In addition to physical and logical risks, human beings may be an additional hazard source. Over the recent past, issues of human security have risen in value (e.g.: revenge acts by dismissed employees, operation disturbances due to inadequate training) (Outpacing change, 2009), but SMEs do not put sufficient weight on these issues. The publication of the ENISA, a professional organisation in the European Union has issued a publication entitled “How to Raise Information Security Awareness”, which provides communication aid for companies. The document makes special mention of obstacles faced by SMEs and defines critical success factors, as is usual in publications of this sort. It is important to make employees understand that information security is not only the responsibility of IT specialists… The creation of information security awareness is perhaps the least cost-demanding issue, yet it is not a simple task but one requiring constant training and “maintenance”.

5. INSTEAD OF CONCLUSION

What can an SME do if it wants information security and has not got the necessary resources?

We strive to answer by modifying and extending Andy Horn’s proposals (Horn, without date):

1. Develop an information security policy and communicate it! Define what business information is important, who has to be able to access it, and in what way.
2. Examine business processes from the perspective of risk. Develop processes to implement and maintain the policy! Appoint persons responsible for information security in each organisation unit.
3. “Centralise” software purchase. Applications should be tested and checked before use (this is particularly true for free downloads…).
4. There should be a constantly updated register of IT devices and databases. Look after physical and data assets!
5. Employees should be kept informed - by formal training, if necessary - the information security tasks that apply to their jobs and make certain they are aware of their responsibility. Strive to keep the “clear desktop, clear screen” rule.
6. Create and implement information management rules, especially in the case of confidential personal and business data. Comply with regulations!
7. Pay attention to physical security, the storage of IT devices and the prevention of unauthorised access to these. Control physical access to information!
8. Ensure business continuity in a crisis or disaster situation! Store important business data redundantly, with the employment of an external service provider, if necessary.
9. Explore and use the information technology possibilities provided by basic and application software (e.g.: log, secrecy).
10. Protect IT and communication systems against malignant software and unauthorised access (e.g.: antivirus, spam filter, and anti-spyware applications)

REFERENCES:

[1]. **Chang, H.; Kim, J.; Lim, S.** (2006) *Information Security Management System for SMB in Ubiquitous Computing.* Lecture Notes in Computer Science, Volume 3983, pp. 707-715

[2]. **Horn, A.**, *Information Security - More Than An IT Challenge for SME.* Available at: www.freshbusinessthinking.com/business_advice.php?CID=3&AID=2629&PGID3 [Accessed 23 November 2009]

[3]. **Park, J.Y.; Robles, R.J.; Hong, C.H.; Yeo, S.S.; Kim, T.** (2008) *IT Security Strategies for SME's,* International Journal of Software Engineering and its Applications, 2(3), July, pp. 91-98

[4]. **Slusariuc, G.** (2004) *Comparative analyse of the SMEs from Romania and European Union,* Annals of the University of Petrosani, Economics, 4, pp.283-288

[5]. **Tawileh, A.; Hilton, J.; McIntosh, S.** (2007) *Managing Information Security in small and Medium Sized Enterprises: A Holistic Approach.* Highlights of the Information Security Solutions Europe, SECURE Conference, Warsaw, (ISSE/SECURE 2007 Securing Electronic Business Processes, pp. 331-339.)

[6]. **Tenner, A.R.; De Toro, I.J.** (1992) *Total Quality Management. Three Steps to Continuous Improvement,* Addison-Wesley Publishing Company, Inc., New York

[7]. **European Network and Information Security Agency - ENISA** (2006) *How to Raise Information Security Awareness (A Users' Guide)*, *June,* Available at: www.enisa.europa.eu/act/ar/deliverables/2006/ar-guide/en [Accessed 24 November 2009]

[8]. **SMB Disaster Preparedness** (2009) *Survey Results*, September, Available at: www.symantec.com/content/en/us/about/media/SMB_Disaster_Recovery_Survey_ Report _Global_2009.pdf [Accessed 1 December 2009]

[9]. **Ernst & Young** (2009) *Outpacing change. 12th annual global information security survey*, Available at: eww.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_ annual_GISS.pdf [Accessed 8 December 2009]

[10]. IT Governance Institute, USA. *CObIT 4.1. Excerpt, Executive Summary, Framework,* Available at: www.itgi.org/ContentManagement/ContentDisplay.cfm?ContentID=50254 [Accessed 12 June 2010]

[11]. IT Service Management Forum (2007), *An Introductory Overview of ITIL V3.* Available at: www.itsmfi.org/files/itSMF_ITILV3_Intro-Overview_0.pdf [Accessed 19 January 2010]

[12]. *ISO27k Toolkit. Version 3.8* (2009) Prepared by the international community of ISO27k implementers at www.ISO27001security.com Available at: www.ISO27001security.com/ISO27k_Toolkit_overview_and_contents_3v8.rtf [Accessed 19 January 2010]