Applicability of ISMS standards in the SME e-commerce sector

Course: 4SA431

Tuesday 7th December, 2010

1 Abstract

The paper formulates several problems related to ISMS implementation in companies running an e-commerce site. It presents probable benefits and costs of such implementation and shows a possible effect of ISMS based on a small case study.

2 Introduction

Security of small e-commerce sites is an extremely interesting topic[1], as is the use of information security frameworks in large enterprises. However, the relationship between the two could be – at first glance – considered a bit problematic: are "thick" methods of security applicable in a lean and cost-constrained environment of a typical SME[2]?

The importance of security in e-commerce is stressed e.g. in [2]: "... information security should be seen as a strategic asset and not as a cost. The increase in a company's e-commerce investment will automatically increase the system's vulnerability to attack; lack of security management measures and policies will result in greater cost." It is also noted that due to inherent dependence on IS/ICT, "e-commerce companies must implement an organizationally validated security management system." However, the steps in the aforementioned book are not feasible for a SME by any means (for example "setting up a team of managers and technical personnel").

The motivation to try to apply ISMS[3] can be best illustrated in the Figure 1. It represents a cyclic ad-hoc approach to security problems, that, however, may seem to be cheaper specifically because it is reactive – the cost comes "later" or "never" (which is also the approach of SME e-commerce in general, where the

[1] The reader is kindly referred to see `http://kohout.se/files/bp.pdf` for a detailed analysis of technical and legal challenges of small e-commerce sites by the current writer.

[2] Small and medium enterprises. For the purposes of the paper, SME is a company with main income from on-line sales with less than 50 employees and turnover less than 50 millions €. This definition is slightly more practical than the one at `http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm`, as on-line sales have much smaller need for large employee base.

[3] Information Security Management System; typically based on a common standard, e.g. ISO/IEC 27001.

largest possible investment is made to acquire customers). Whether an economically sustainable and more systematic approach based on ISMS is possible and feasible is the topic of this paper.

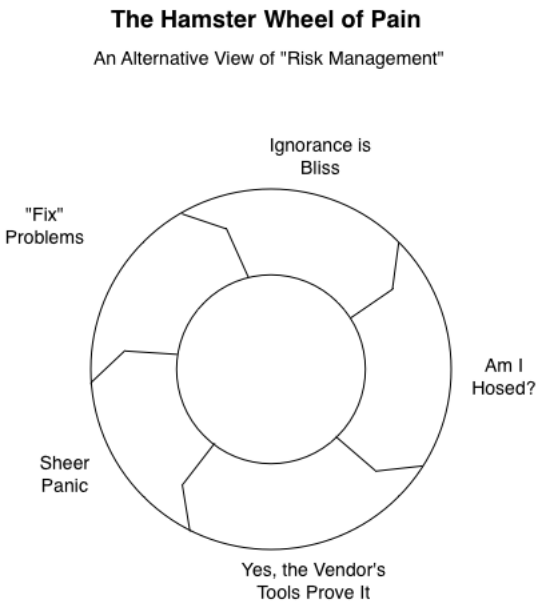

Figure 1: Hamster wheel of pain. Source: [1].

3 Why information security

For SME's, the main reasons for deploying security measures can be (roughly) divided into three areas: prevention of direct damage to the organization (e.g. disputed credit card transactions due to identity theft), protection of business data and protection of data required by the law (or contracts)[2]. The need to prevent direct damage is usually well understood and ad-hoc controls to prevent it are usually in place (ie. order confirmation by telephone, outsourcing[4] of credit cart processing etc.)

[4] Outsourcing – with appropriate legal paperwork – is a reasonable way to solve many threats to company assets ("transferring the associated business risks to other parties, e.g. insurers, suppliers." in [7, 4.2.1 e) 4)]

The need to protect business data may be well understood in certain areas (contracts, credit card data, supplier information), but ignored in others (e.g. which data about site visitors can be released). The protection of data required by the law is usually accomplished only in a theoretical, formal way (registering as a processor of private data). The last two categories usually exist in a combined, inseparable way – e.g. a database of customers' email addresses can be considered business data (asset); however, every single email address is also[5] private data, therefor a liability. The same applies to most data concerning customers (e.g. visitors statistics); for a complete list, see Appendix A.

The general benefits of an ISMS for an organization can be summarized as follows (paraphrased according to [2]):

1. Predictability and quantifiability of the potential loss from the possible threat of the current information system operation (including better understanding of risks).
2. Improvement of "the stability, effectiveness, efficiency and reliability of the organization's assets."
3. Improved security awareness.
4. Support of decision making (establishment of priorities and cost/effectiveness ratios).
5. Improvement of public trust and competitiveness through government certification.
6. Improvement of corporate image due to certification.
7. Substantial "support of the corporate goal."

4 Common security problems in SME's

The basic problem is a significant lack of resources (financial, human). The common approach to security is nicely shown in a model in the Figure 2

[5] At least in the European Union.

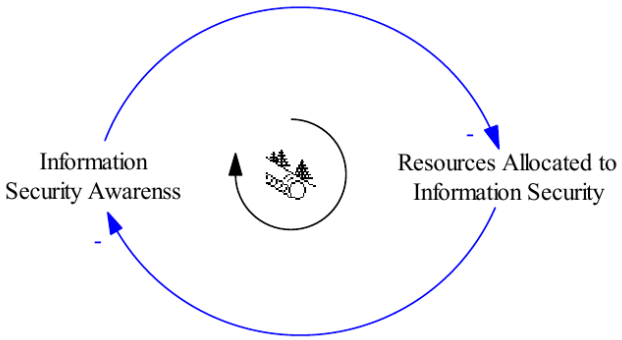

Figure 2: Negative feedback. Source: [4].

The negative feedback lowers the amount of money available for security (based on the assumption that a small company cannot afford security, because it's not a likely target). The feedback continues: the less aware we are about security problems, the less we invest and the less we invest, the less we know about security. "Even with appropriate awareness and complete understanding of the security issues, SME's do not possess the required resources (human, monetary or technical) that should be invested to solve the problem. SMEs typically operate under very tight budgets;have seriously limited manpower and many needs competing for a very limited supply of resources, leading to information security being pushed down the priorities list."[4] Another problem is the bi-dimensionality[4] of information systems security – both the technical aspect (correct algorithms, cryptography,...) and social factor is present and specifically in SME's with less documented and less rigid processes, the social factor becomes more important.

Other issues have been highlighted in [3]: "the gap between the current state of an SME and the state to reach for the certification" (many management systems in SMEs are developed from ground up). Only a limited set of formalized documents and policies exist[6]; the same applies to human resources – users in SME's generally need more training during the implementation phase of the ISMS.

[6]In [3], Codasystem, a provider a software directly related to computer security (integrity and non-repudiation of documents), is mentioned as an example of a company with the lack of formal policies – which, in the opinion of the current writer, shows that probably other companies, not directly related to computer security, would have even more problems and even less documentation.

5 Possible direct benefits of ISMS

For SME's, the most beneficial outcome of an ISMS is the system itself. Typically, the working environment of SME's is relatively informal, with very broadly defined responsibilities; ISMS mandates documentation, which vastly improves both accountability for any action and replace-ability of employees[7]. An indirect benefit is a better contact with industry best practices, which can inspire the company pro improve processes in other areas.

A very practical example is control and ownership of domain names. Domain names are extremely critical part of company infrastructure[8], yet in SME's, their ownership (mandated in [7, A.7.1.1, A.7.1.2] as "Inventory of assets"[9] and "Ownership of assets"[10]) is sometimes unclear and due to periodical renewal, it is not uncommon to simply forget to renew a domain name (due to lack of clearly defined responsibilities). The author has encountered a company, where the firm's domain name was owned by one of its employees – and when the employee had been made redundant, she used the domain name as leverage to solicitate for money (violation of "Return of assets"[7, A.8.3.2][11]). Another example is when the original domain name has been purchased by then self-employed friend of current company owner. Over time, the self-employed friend started his own firm as a legal entity and lost control over the original email address, used to register the domain. The result is a domain name owned by an individual completely unrelated to the company, and the email address, associated with the domain name, no longer exists and is under control of a former ISP[12].

A security policy for information exchange ([7, A.10.8.1]) would also greatly improve security of SME's, as it would lower the reliance on insecure plaintext

[7] E.g. in case of illness.

[8] In case of e-commerce companies, probably the most critical part as anything else can be substituted to some extent.

[9] "All assets shall be clearly identified and an inventory of all important assets drawn up and maintained."

[10] "All information and assets associated with information processing facilities shall be 'owned' 3) by a designated part of the organization."

[11] "All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement."

[12] Which greatly complicates any manipulation with DNS records and endangers domain ownership should the ISP reuse the email account.

protocols (ie. email, [7, A.10.8.4][13]) and informal authority ("the boss says...") The clauses (A.10.9.1: Electronic commerce, A.10.9.2: On-line transactions and A.10.9.3: Publicly available information), related to e-commerce can be employed to improve perception of security (and thus customer trust and turnover)[14].

Implementation of an ISMS is also a possibility to improve physical security, especially "barriers such as walls, card controlled entry gates or manned reception desks"[7, A.9.1.1]. Backup plans should not be underestimated either – in SME's, automatic backups are often employed for server data only. Workstations may or may not be backed up at random, laptops very rarely and at the responsibility of the user ([7, A.10.5.1], Information back-up).

6 Possible issues and scalability of ISMS in SME

There exist several issues of ISMS that could counter any benefits that such systems offer to the company.

The main problem, high resource requirements relative to low (perceived) utility of the system, can be overcome by two different approaches. The first is finding cost-saving possibilities within the certification framework and by finding possibilities to improve the overall inner processes of the company. The second is limiting the standard, for example by applying a set of modifications to the original standard, as suggested in [3][15] (paraphrased):

1. Downsize the requirements in order to reduce the cost and the complexity of an ISMS.

2. Smoothen the approach to the users (ISMS as possibility, not a constraint).

3. Give the major recommendations and generic tasks to ensure the proper operation of the ISMS.

[13] Information involved in electronic messaging shall be appropriately protected.

[14] Anecdotal evidence: in the US with a more developed e-commerce market, most sites boast with "security stickers" (logo's of known companies or mangled phrases – "128 bit encryption"). Compare to the situation in the Czech Republic.

[15] The paper [3] is a part of larger study; several outcomes (recommendations for SMEs) can be found at: `http://www.cases.public.lu/fr/index.html`, `http://www.cases.public.lu/fr/pratique/oldental/index.html`.

4. Provide implementation guidance for each process of the PDCA cycle.

5. Ensure coherence and reliability of (this) tailored handbook.

6. Provide tool support. A framework of documentation tools and templates should be proposed as a support for the implementation.

Such a downsized system would be hardly certifiable ("Excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard."[7, 1.2], also required as "Independent review of information security"[7, A.6.1.8]). Despite the unverifiability, such system still provides more security than no system (a similar approach could be to use some of the NIST publications, aimed at SME's). However, the author believes that any information security management system would, without external audit, lose any credibility[16] after a relatively short period of time (the 3 years time limit in [7] could be considered also as a time period after which a self-certified ISMS completely disintegrates). The downsized system can also be employed as a first step towards a real, more rigid ISMS, to smoothen the transition (there are attempts to provide such intermediate system, e.g. in [5]).

As for minor problems, "security in third party agreements"[17][7, A.6.2.3] pose a significant problem. With SME's low-cost operations, agreements typically don't contain a an SLA agreement with refunds comparable to possible losses (e.g. the SLA for a leased server is only covered up to the fee paid monthly, while the possible loss to the company is larger by several orders of magnitude).

7 Case study

The current writer would like to present a case study of an information security incident[18], completely preventable had an ISMS been deployed.

[16] Theory of broken windows applies[9].

[17] "Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements."

[18] "a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"[7, 3.6]

The incident happened to an undisclosed e-commerce site, which had to be transfered to a new server due to an unexpected amount of visitors (result of a very successful Christmas advertisement campaign). The move was planned to happen during the weekend at night; because of the new server, the unique opportunity was used to upgrade certain server software (the most critical part: PHP 5.2.6 to PHP 5.3.4). Before the transfer, new configuration had been extensively tested as to whether the e-commerce software after the transfer would support the same *business functionality* as before the transfer[19].

After a seemingly extremely successful migration with less than 5 minutes downtime on Sunday at around 3 a.m., nothing seemed to be out of ordinal. On Monday noon, it has been discovered by the system administrator that Postfix[20] was sending several several thousand emails *per minute* (see Figure 3). The logs explained even more (Figure 4).

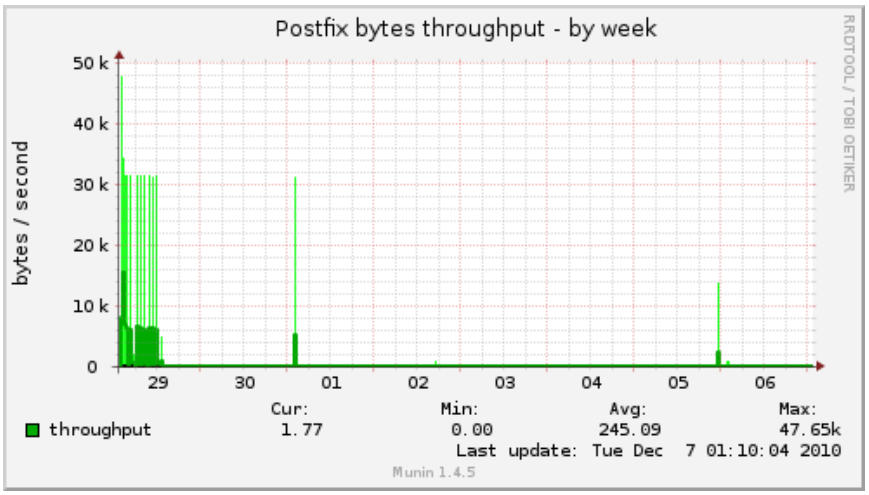

Figure 3: Postfix (email server) throughput, graphs generated by Munin. Source: author.

The outgoing emails were actually spam. Such incident is extremely hazardous to an e-commerce company that directly relies on a successful delivery of email (especially confirmation of an order – and if the IP address of the server is associated

[19]Through automated tests, user tests and log checking.
[20]Mail transfer agent.

```
...
Nov 29 02:27:22 xyz postfix/smtp[21303]: E018588B3F: to=<Brodkidd@aol.com>, relay=mailin-04.mx.aol.com[205.188.146.194]:25,
 conn_use=3, delay=1.5, delays=0.07/1/0.09/0.28, dsn=5.1.1, status=bounced (host mailin-04.mx.aol.com[205.188.146.194]
 said: 550 5.1.1 <Brodkidd@aol.com>: Recipient address rejected: aol.com (in reply to RCPT TO command))
...
Nov 29 02:27:46 xyz postfix/smtp[21312]: 24FBF88C02: to=<builder4life@aol.com>, relay=mailin-04.mx.aol.com[64.12.138.161]:25,
 delay=6.4, delays=0.06/4.5/1.3/0.59, dsn=4.2.1, status=deferred (host mailin-04.mx.aol.com[64.12.138.161] said: 421 4.2.1
  MSG=:  (DYN:T1)  http://postmaster.info.aol.com/errors/421dynt1.html  (in reply to end of DATA command))
...
Nov 29 02:27:46 xyz postfix/smtp[21339]: 34A8788C04: to=<buildingblks@aol.com>, relay=mailin-02.mx.aol.com[64.12.90.65]:25,
 delay=6.5, delays=0.08/4.4/1.2/0.81, dsn=4.2.1, status=deferred (host mailin-02.mx.aol.com[64.12.90.65] said: 421 4.2.1
MSG=:  (DYN:T1)  http://postmaster.info.aol.com/errors/421dynt1.html  (in reply to end of DATA command))
...
```

Figure 4: Postfix (email server) logs. Source: author.

with sending spam[21], it will very soon appear on blacklists[22]). The root cause was a minor incompatibility in PHP versions and a silenced exception in a CAPTCHA module (so it did not work properly and allowed sending spam through a form on the e-commerce site). It took less than 24 hours for an automatic web crawler to discover and abuse the vulnerability.

Several requirements of a common ISMS (e.g. based on ISO/IEC 27001) had been violated. The tests before the transfer focused on *business functionality* (ie. "what should work"), not on security ("what should not be possible")[23]. No direct and clear responsibilities were set ([7, A.6.1.3][24] and no formal, *verified* migration plan had been followed ([7, A.6.1.4][25], [7, A.10.3.2][26] and the most important, [7, A.12.1.1][27], [7, A.12.5.2][28]).

With a correctly defined, implemented and certified information security management system, the security incident would have been completely preventable.

[21] Not withstanding possible legal repercursions.

[22] The remedy is to change IP address of the server.

[23] "g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls"[7, 4.3.1]

[24] "Allocation of information security responsibilities"

[25] "A management authorization process for new information processing facilities shall be defined and implemented."

[26] "Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance."

[27] "Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls."

[28] "When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security."

8 Conclusion

The current writer believes that information security management systems, based on international standards (e.g. ISO/IEC 27001), are readily applicable in the SME sector (specifically, e-commerce, or any sector largely dependent on IS/ICT). However, the rate of adoption will continue to be relatively slow not due to the standard itself, but due to limited knowledge and experience with the use of ISMS in a budget-constrained environments of a typical SME. The potential of ISMS in SME would be greatly improved if a central body (e.g. government, European Union institutions) provided a pre-packed extended documentation and typical scenarios for deployment in the sectors of economy most vulnerable to attacks based on compromising IS/ICT.

A Definition of assets

A simplified list of assets (most physical assets are omitted); adapted from [7].

- Tangible assets:
  - server hardware and networking equipment required to run the site
  - computer hardware used to administer the site
  - other assets not related to the actual site (warehouse, office building, etc.)
- Intangible assets
  - e-commerce site software ("shopping cart"), its customization
  - design of the site
  - domain name
  - DNS records
  - site email accounts[29]
  - product database (structured list of products with current prices)
  - orders database (typically required to be immutable)
  - customer database (addresses, credit cards, relation to orders)
  - third party software related to the site (affiliate software, accounting software import modules, visitor tracking software)
  - advertisement data
  - visitors statistics, tracking database
  - customer trust, brand name
  - customer-created content (e.g. product comments, ratings)

[29]Email accounts will not be described in the thesis as they are not related to the actual e–commerce site. However, isolating the email server (or provider) from the site is sensible in case of downtime – by using one provider for the site and another (geographically separated) for emails, the chance that at least one system will be accessible by customers can be increased. Data security (especially legal liabilities) must be taken into account in case of outsourcing outside Europe.

- search engine results ranks for important keywords
- money stored in pre-paid services (e.g. AdWords)
- server and networking equipment software required to run e-commerce site software[30]
- other software and data not directly related to the site.

Note: reused as a reference; first appearing in the authors' bachelors thesis.

[30] Expected to be outsourced, and thus out of the scope of the thesis.

B Private data protection

95/46/EC, Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

   Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

   - the processor shall act only on instructions from the controller,
   - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Source: [8]

Note: all links were accessible between 21^{st} November 2010 and 7^{th} November 2010.

References

[1] Jaquith, A., *Security Metrics: Replacing Fear, Uncertainty, and Doubt.* Addison-Wesley Professional, 2007. ISBN 978-0-321-50947-5.

[2] Gallegos, F., Senft, S., Manson, D. P., Gonzales, C., *Information technology control and audit.* Auerbach Publications, 2004, second edition. ISBN 978-0849320323.

[3] Valdevit T., Mayer N., Barafort B., *Tailoring ISO/IEC 27001 for SMEs: A guide to implement an Information Security Management System in small settings.* Communications in Computer and Information Science, 1, Volume 42, Software Process Improvement, Part 6, Pages 201-212. URL: `http://www.springerlink.com/content/k2843071645420k1/fulltext.pdf`.

[4] Tawileh A., Hilton J., McIntosh, S., *Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach.* 2007, ISSE/SECURE 2007 Securing Electronic Business Processes, Part 4, Pages 331-339. URL: `http://www.springerlink.com/content/j938426378g4617k/fulltext.pdf`.

[5] Sánchez L. E., Santos-Olmo A., Fernández-Medina E., Piattini M.,*Managing Security and its Maturity in Small and Medium-sized Enterprises.* Journal of Universal Computer Science, vol. 15, no. 15 (2009), 3038-3058. URL: `http://www.jucs.org/jucs_15_15/managing_security_and_its/jucs_15_15_3038_3058_sanchez.pdf`

[6] Doucek, P., Novák, L., Svatá, V., Nedomová, L.: *Řízení bezpečnosti informací.* Professional Publishing, Praha, 2008. ISBN 978-80-86946-88-7.

[7] *ISO/IEC 17799-2005: Information technology – Security techniques – Code of practice for information security management.*. International Organization

for Standardization, Geneva, Switzerland. URL: http://www.iso.org/iso/catalogue_detail?csnumber=39612.

[8] *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[9] James Q. Wilson and George L. Kelling *Broken Windows*. The Athlantic Monthly, březen 1982, http://www.manhattan-institute.org/pdf/_atlantic_monthly-broken_windows.pdf.