# *Information Security in Small and Medium-Sized Companies*

## *Bezpečnost informací v malých a středních firmách*

**DAVID KRÁL**

**Abstract**

Information security doesn't involve only large organizations. Small and medium-sized companies must closely examine this issue too, because they are increasingly threatened by cyber attacks. Many of them mistakenly believe, that security of their valuable data is sufficient, or that the attackers are not interested in them. Existing standards and methodologies for implementation and management of information security are often hard to transfer to the environment of small and medium-sized businesses, because these companies do not want, or are not able to observe a large bounty of prescribed procedures and regulations related to certification standards. The article offers a methodology of balanced information security for small and medium-sized businesses. It describes important areas of information security and defines the basic criteria for assessing the security quality of each of the key areas.

**Keywords**

information security, small and medium-sized businesses, risk management, key assets, security of processes, human resources, security incidents.

**Abstrakt**

Bezpečnost informací se netýká pouze velkých organizací. Také malé a střední firmy se musí touto problematikou intenzivně zabývat, protože se stále častěji stávají terčem kybernetických útoků. Mnohé se mylně domnívají, že zabezpečení jejich cenných dat je dostatečné, nebo že se o ně útočníci nezajímají. Stávající standardy a metodologie pro zavádění a řízení informační bezpečnosti není často možné jednoduše aplikovat do prostředí malých a středních firem, protože tyto firmy nechtějí, nebo nejsou schopné dodržovat velké kvantum předepsaných procedur a předpisů spojených s certifikací normy. Článek nabízí metodiku vyvážené informační bezpečnosti pro malé a střední firmy. Popisuje důležité oblasti informační bezpečnosti a definuje základní kritéria pro posouzení kvality zabezpečení každé z klíčových oblastí.

**Klíčová slova**

bezpečnost informací, malé a střední firmy, analýza rizik, klíčová aktiva, bezpečnost procesů, lidské zdroje, bezpečnostní incidenty

## Introduction

Quality security of sensitive data and key assets becomes now a question of absolute necessity for a company of any size and orientation. History of evolution of information security began particularly in environment of large organizations that processed a large amount of data. It is logical that it was larger and richer companies which often have sufficient resources to invest in the security of their assets. Moreover, relatively large percentage of small and medium-sized businesses has about the security of its information somehow faulty ideas. As stated in the survey of McAfee´s 2008[1], more than half of the 1100 respondents of companies from the U.S. and European small and medium-sized companies think, that only large organizations can be targets of cyber attacks. The opposite is true. More and more attackers are focusing on mid-sized organizations, which are insufficiently protected and they find it much easier to get to their sensitive data.

Information security in large companies is generally dealt with certification[2], which to some extent, guarantees a certain quality of security and ensures a certain consistency with other management systems of organization. Small and medium-sized companies are often preventing the implementation of certified standards. The reason is the fear of heavy formal administration, which is often required for certification, but is mainly for small businesses unnecessary and burdensome. For medium-sized organizations (50-200 employees), the certain administration associated with information security is a necessity. Employees, as in small businesses, are familiar with each other, but already there is a certain degree of anonymity, which may trigger the fact that some employees will not respect security procedures, especially if they are not precisely defined, and compliance will not be regularly checked. The certification is generally recommended for these organizations, but each company must be evaluated individually. It depends on several circumstances, whether the certification is appropriate for the organization or the establishment of their internal methodology for information security.

## 1 Balanced information security

Methodology of balanced information security, which is the subject of this article, is primarily proposed for small and medium-sized businesses. Its aim is to define the most important and absolutely necessary criteria for information security so that the system meets the requirements of a comprehensive solution of the issue. On the other hand, it seeks how to minimize the administrative burden for these organizations, which is, as mentioned above, one of the main reasons, why companies hold a negative attitude to the most widespread certifications.

An essential step in establishing of any system of information security is a risk analysis. Without identifying the key assets of the organization, determine threats and vulnerabilities that may adversely affect these assets and without setting the basic security policy, how will the company effectively protect its important assets, it is impossible to implement and manage an effective system of information security in the organization of any kind and size.

1 *McAFee (2008).*

2 *e.g. ISO/IEC 27001 (2005).*

The methodology is concerned with the definition of basic criteria for the protection of the main processes and technologies in the organization, including in particular the field of physical security, secure communications and access control.

The issue of human resources is considered as a key area. In many statistics there is indicated that a large percentage of security incidents and losses of sensitive data is being caused by intentional or unintentional human error factor.

If any security incident occurs, it is considered desirable, that losses, which occur as a result of any fault, were the least possible. In this case is appropriate, when security incident is quickly removed and that interested staff is more clever next time and is able to avoid it. The management of security incidents is concerned with these issues and it is also a part of the methodology.

Methodology considers it appropriate to take into account the extent of reliance on information and communication technologies when assessing the quality criteria of information security in organization.

If the information security of a company should be considered as a balanced one, it must hold true, that all circuits of the system are above an average level, and none of the monitored area has a significant vulnerability, that would significantly degrade the entire system (information security is at a level of its weakest point)[3].

The whole process is divided in 5 steps, which analyze the current level of data security in the organization, changes are proposed in the non-secure areas. These changes are applied and then it is determined whether these changes contributed to the improvement of the system of information security of observed organization.

## The phases of a balanced information security in a company:

**1) Pre-audit of organization**
The first step of the proposed methodology is to evaluate the existing information security of a company. It consists of evaluating the quality of information security solutions in key areas of information security system and determining the rate of dependence of the organization on information technologies.

**2) Interpretation of the results found**
On the basis of pre-audit the particular areas of information security are divided into three groups according to points obtained:

- insufficient protection,
- protection requiring improvements,
- adequate protection.

**3) The proposed solution**
If the protection is assessed as insufficient, a proposal for a complete change in approach to the area follows.

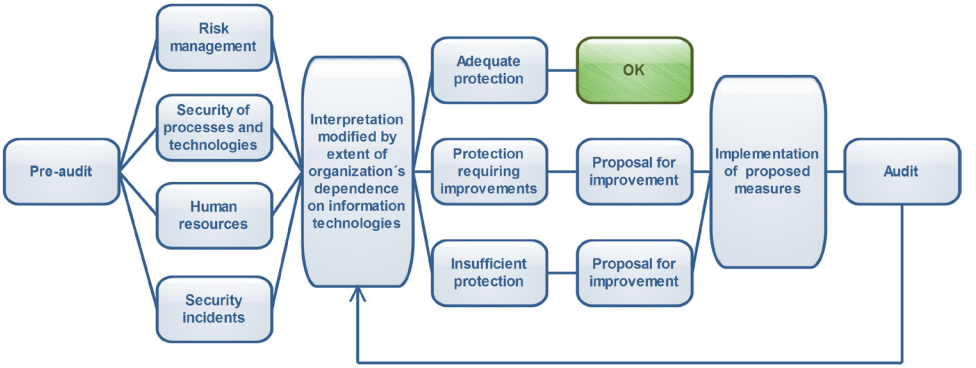
3 *ANDERSON (2008).*

If the protection is assessed as requiring improvements, the steps are proposed to enhance the efficiency of the information security area, while maintaining the existing policy.
If the protection is assessed as adequate, it is not necessary to change existing one or introduce new security measures.

**4) Implementation of the proposed solutions**
The proposed measures are according to financial and time possibilities integrated into the organization's processes as soon as possible.

**5) Audit**
Re-audit of the quality of company's information security is conducted. Benefits of the newly introduced security measures are assessed. If the new interpretation of the results finds that some deficiencies have not been remedied, the new solution draft follows.
The proposed approach is shown schematically in the following figure.

**Figure 1:** Methodology of a balanced information security




*Source: own research.*

## 2 Pre-audit of organization

### Dependence of organization on information technologies

The first step in the process is to determine how the organization is dependent on information technologies. Determination of this dependence is very important, because a different level of security will be expected in the organization, which is more or less independent on the information technologies than in the organization, which is vitally dependent on these technologies.
Dependence is determined on the basis of the following criteria:

1. Annual budget (0 – less than 1 mil., 4 – more than 100 mil.)
2. Number of employees (0 – less than 20, 4 – more than 200)
3. Dependence on information and communication technologies to offer products and services to customers
4. Value of organization's intellectual property stored or transmitted in electronic form
5. Impact of information system downtime on operations

6. Impact to organization's operations from an Internet outage
7. Partner and customer sensitivity to security and privacy
8. Potential impact on reputation of a serious security incident
9. Extent of operations dependent upon third parties
10. Extent of sensitive data/property that may become a target of a violent physical or cyber attack

Each criterion is graded in the range 0-4 and the organization's dependence on information technologies is identified according to the following table:

**Table 1:** Dependence on information technologies

| Rating/Criterion | Rating/Spread | Level |
|---|---|---|
| 0 | 0-8 | Very low |
| 1 | 9-16 | Low |
| 2 | 17-24 | Middle |
| 3 | 25-32 | High |
| 4 | 33-40 | Very high |

*Source: own research*

## Risk Management

The next step of the pre-audit is to assess various areas of organization's information security management. The first of these areas is risk management. It is observed what strategy for the information security is used. This area is considered as a key one, the appropriate protection requires implementing more criteria than in other areas of research.

The level of quality of this area is determined on the following criteria:

1. Does the organization formulated a document called information policy?
2. Was the risk analysis accomplished in the organization in the last 2 years to identify the assets that need protecting?
3. Does the organization use self specialist / qualified external company / special software for risk analysis?
4. Has the organization determined the relationship between key assets and processes depending on them?
5. Has the organization identified security threats associated with key assets?
6. Was the analysis of vulnerability accomplished, i.e. determining vulnerabilities that could be used by identified threats?
7. Is the loss of every key asset assessed in the organization?
8. Is the security strategy documented which establishes procedures to keep the risks to an acceptable level?
9. Is the security strategy documented which includes plans for the future to reduce the risks associated with key assets?
10. Is this strategy updated at least once a year?

Each criterion is graded on a scale of 0-4 and a level of implementation is assigned - see Table 2.

**Table 2:** Risk management – the level of implementation

| Rating | Level |
|---|---|
| 0 | Not implemented |
| 1 | Planned |
| 2 | Partially implemented |
| 3 | Just before implementation |
| 4 | Fully implemented |

*Source: own research.*

Based on the results, the level of protection of this area is determined upon the previously identified dependence of the organization on the information technology as shown in the Table 3.

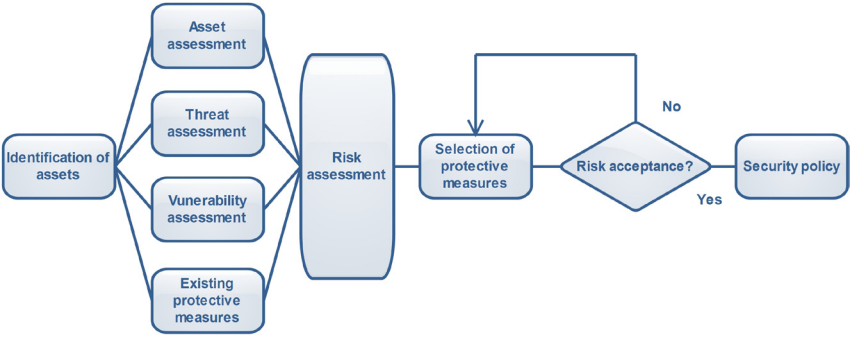
**Table 3:** Risk management - rating

| Dependence on IT | Rating | Interpretation |
|---|---|---|
| Very low | 0-13 | insufficient protection |
| | 14-23 | protection requiring improvements |
| | 24-40 | adequate protection |
| Low | 0-16 | insufficient protection |
| | 17-26 | protection requiring improvements |
| | 27-40 | adequate protection |
| Middle | 0-19 | insufficient protection |
| | 20-29 | protection requiring improvements |
| | 30-40 | adequate protection |
| High | 0-22 | insufficient protection |
| | 23-32 | protection requiring improvements |
| | 33-40 | adequate protection |
| Very high | 0-25 | insufficient protection |
| | 26-35 | protection requiring improvements |
| | 36-40 | adequate protection |

*Source: own research.*

The following diagram shows a possible procedure for the implementation of risk management system.

**Figure 2**: Risk management - diagram




*Source: own research.*

## Security of processes and technologies

The next step in the organization's audit is the essential safety inspection of running processes and technologies related to information security. This includes in particular the field of physical security, secure communications and access control.

The level of this area is assessed by the following criteria:

1. Are spaces that contain equipment for the processing of information, protected by safety perimeters / barriers?
2. Are the organization's facilities, which contain sensitive information or equipment accessible only to authorized persons?
3. Is the organization protected against any external or natural threats, a power failure?
4. Are devices that process information, protected from power failure and from other forms of interruption caused by failures of support facilities?
5. Is there a procedure for the safe dismantling and disposal of assets after the authorization of the authorized person not allowing sensitive data to escape?
6. Are all stations in the organization sufficiently protected against malicious programs and codes?
7. Is there a regular and secure backup of data in the organization?
8. Are confidential, personal or sensitive data encrypted and associated encryption keys properly protected?
9. Are all the software and the exchange of information within the organization or in an exchange with external partners adequately protected?
10. Are contracts with organization's partners supplying products/services provided with a list of security measures and sanctions, if partners do not comply with these measures?
11. Are the activities of all users, exceptions, and events related to security of information stored in the information system of organization for a sufficiently long period of time?
12. Are found data analyzed and appropriate measures to eliminate errors adopted?
13. Is a clean desk policy and screens respected in the organization?
14. is there a procedure for registering a user to the information system of the organization and the allocation of rights to access to the certain areas of information system?
15. Do all users of the information system have an unique identifier (ID) so that a responsibility for their actions can be traced?
16. Are all users forced by the system to create only so-called strong passwords?
17. Are special procedures applied in the case of remote authentication access to the organization's information system?
18. Are the ports for remote diagnostics and configuration securely protected?
19. Are all stations after a predetermined period of inactivity logout from the system?
20. Are there policies and procedures for safe work on mobile computing devices and equipment in the organization?

Each criterion is graded on a scale of 0-4 and a level of implementation is assigned - see Table 4.

**Table 4:** Security of processes and technologies – the level of implementation

| Rating | Level |
|---|---|
| 0 | Not implemented |
| 1 | Planned |
| 2 | Partially implemented |
| 3 | Just before implementation |
| 4 | Fully implemented |

*Source: own research.*

Based on the results, the level of protection of this area is determined upon the previously identified dependence of the organization on the information technology as shown in the Table 5.

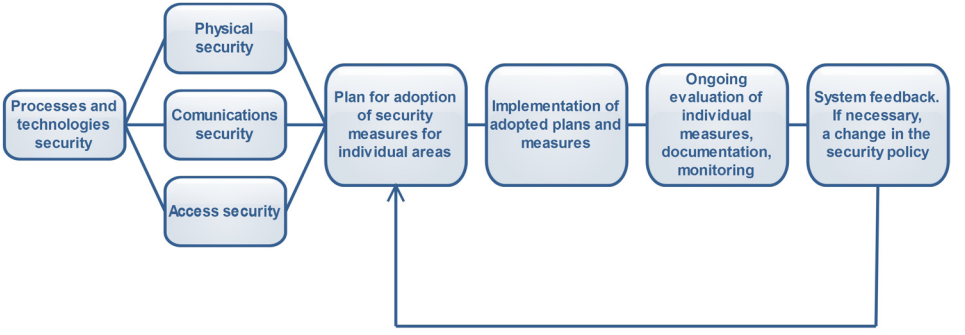
**Table 5:** Security of processes and technologies - rating

| Dependence on IT | Rating | Interpretation |
|---|---|---|
| Very low | 0-20 | insufficient protection |
| | 21-40 | protection requiring improvements |
| | 41-80 | adequate protection |
| Low | 0-26 | insufficient protection |
| | 27-49 | protection requiring improvements |
| | 50-80 | adequate protection |
| Middle | 0-34 | insufficient protection |
| | 35-57 | protection requiring improvements |
| | 58-80 | adequate protection |
| High | 0-42 | insufficient protection |
| | 43-63 | protection requiring improvements |
| | 64-80 | adequate protection |
| Very high | 0-50 | insufficient protection |
| | 51-67 | protection requiring improvements |
| | 68-80 | adequate protection |

*Source: own research.*

The following diagram shows a possible procedure for the implementation of processes and technologies security.

**Figure 3:** Security of processes and technologies - diagram




*Source: own research.*

## Human resources

The human factor undoubtedly brings the highest risk for information security management. Various sources confirm that about 80% of all security incidents are caused by human error. At this stage is examined how the organization manages the area of human resources in the context of enforcing information security.

Quality level of this area is assessed on the basis of these criteria:

1. Is the person / service / external company defined in the organization, whose primary task is the management of information security?
2. Does this subject report periodically to the managers of the organization about observance of the rules and effectiveness of established security policy?
3. Does each employee have a clearly defined role and responsibilities within the security policy of the organization?
4. Is this responsibility included in the employment contracts of all employees?
5. Are the previous activities of applicants for employment reviewed in the organization in relation to their ability to work well with sensitive information they will be responsible for?
6. Are trainings for staff and users of third parties relating to information security policy regularly organized?
7. Does the organization have the disciplinary process for employees who have violated security policy and caused a security incident?
8. Is the responsibility for termination of employment or changing jobs clearly defined in the organization?
9. Is in the contract clearly defined, the employee is obliged to return all assets he/she could dispose with and was responsible for before the end of employment?
10. Are all access rights in the organization withdrawn automatically to all outgoing employees?

Each criterion is graded on a scale of 0-4 and a level of implementation is assigned - see Table 6.

**Table 6:** Human resources – the level of implementation

| Rating | Level |
|---|---|
| 0 | Not implemented |
| 1 | Planned |
| 2 | Partially implemented |
| 3 | Just before implementation |
| 4 | Fully implemented |

Based on the results, the level of protection of this area is determined upon the previously identified dependence of the organization on the information technology as shown in the Table 7.

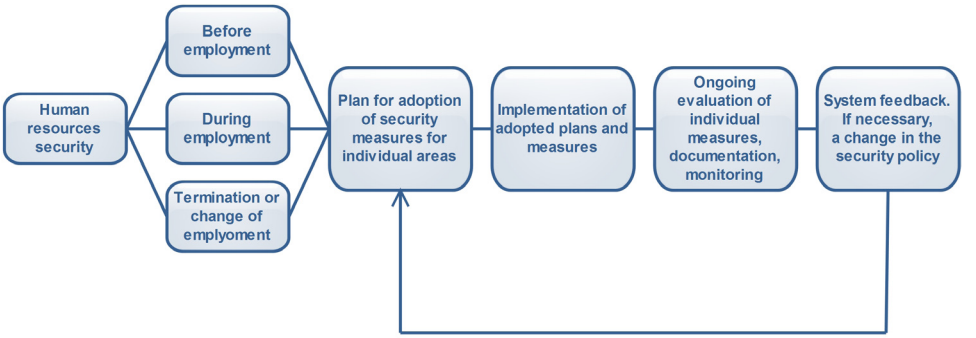
**Table 7:** Human resources security - rating

| Dependence on IT | Rating | Interpretation |
|---|---|---|
| Very low | 0-10 | insufficient protection |
| | 11-20 | protection requiring improvements |
| | 21-40 | adequate protection |
| Low | 0-13 | insufficient protection |
| | 14-24 | protection requiring improvements |
| | 25-40 | adequate protection |
| Middle | 0-17 | insufficient protection |
| | 18-28 | protection requiring improvements |
| | 29-40 | adequate protection |
| High | 0-21 | insufficient protection |
| | 22-31 | protection requiring improvements |
| | 32-40 | adequate protection |
| Very high | 0-25 | insufficient protection |
| | 26-33 | protection requiring improvements |
| | 34-40 | adequate protection |

*Source: own research.*

The following diagram shows a possible procedure for the implementation of human resources security.

**Figure 4:** Human resources security - diagram




*Source: own research.*

## Security incidents

If the safety incident occurs in the organization in spite of all precautions, it is important to be unveiled as soon as possible and caused the minimum damage.
At this stage is determined what methodology the organizations uses to detect, identify and resolve security incidents.

The following criteria determine the quality of the security area:

1. Is there a company document that defines and classifies the potential security events and security incidents that may occur in the organization?
2. Are all employees required to report any observed vulnerability in the organization´s information system, which could mean the creation of a security incident?
3. Are there regular trainings for all staff and participants of third parties in the organization, on which the level of safety awareness is increased to all participants?
4. Are all employees instructed how to report about a security incident to the responsible person / department in the organization after detecting it?
5. Are the responsibilities and procedures for the rapid resolution of a new incident clearly defined in the organization?
6. Are there mechanisms to quantify the types and extent of security incidents emerging in the organization?
7. Are there mechanisms for quantifying the costs incurred related to the removal of security incidents in the organization?
8. Is there an evidence of occurred security incidents collected and stored to be used by the criminal justice proceedings?
9. Are there risk scenarios in case of unexpected or intractable security incident?
10. Are security incidents regularly evaluated and the findings towards risk analysis or security incidents management accepted?

Each criterion is graded on a scale of 0-4 and a level of implementation is assigned - see Table 8.

**Table 8:** Security incidents – the level of implementation

| Rating | Level |
|---|---|
| 0 | Not implemented |
| 1 | Planned |
| 2 | Partially implemented |
| 3 | Just before implementation |
| 4 | Fully implemented |

*Source: own research.*

Based on the results, the level of protection of this area is determined upon the previously identified dependence of the organization on the information technology as shown in the Table 9.

**Table 9:** Security incidents - rating (part 1)

| Dependence on IT | Rating | Interpretation |
|---|---|---|
| Very low | 0-10 | insufficient protection |
| | 11-20 | protection requiring improvements |
| | 21-40 | adequate protection |
| Low | 0-13 | insufficient protection |
| | 14-24 | protection requiring improvements |
| | 25-40 | adequate protection |
| Middle | 0-17 | insufficient protection |
| | 18-28 | protection requiring improvements |
| | 29-40 | adequate protection |

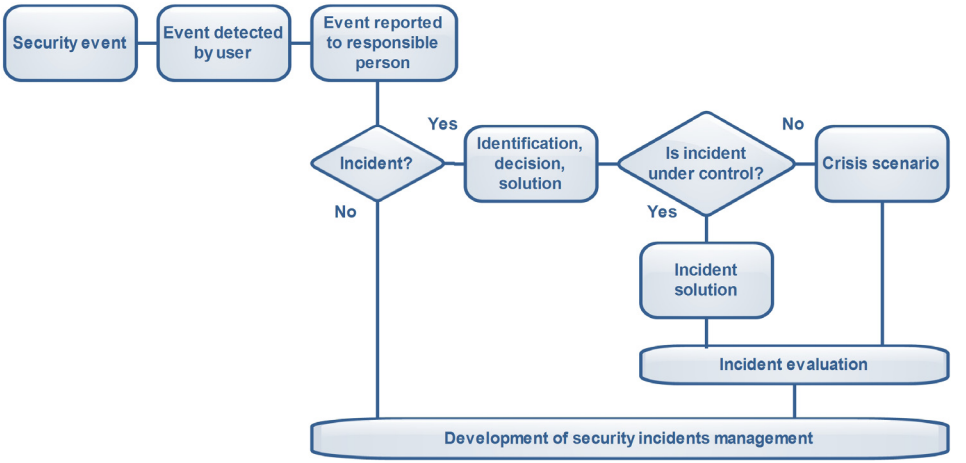
**Table 9:** Security incidents - rating (part 2)

| Dependence on IT | Rating | Interpretation |
|---|---|---|
| High | 0-21 | insufficient protection |
| | 22-31 | protection requiring improvements |
| | 32-40 | adequate protection |
| Very high | 0-25 | insufficient protection |
| | 26-33 | protection requiring improvements |
| | 34-40 | adequate protection |

*Source: own research.*

The following diagram shows a possible procedure for the implementation of human resources security.

**Figure 5:** Security incidents - diagram




*Source: own research.*

## Conclusion

It is very difficult to develop a standard for information security management, which would suit the entire spectrum of organizations. Recently formed standards could meet a wide range of users, because they are more flexible and offer more space for the selection of measures applied. But I dare say that there will always be special cases, which will require special approach and these cases are much more likely to occur within small and medium-sized businesses. On the other hand, I think, it is possible to define the most important areas of information security, which should not be forgotten in the security policy of any organization. This article tries to describe these areas and also specifies the basic criteria in each of these areas. If they are applicated, a sufficient level of security can be guaranteed and key assets of organization are adequately protected.

The methodology is a guide to analyze the quality of information security. If the audit of the organization indicates that some of the areas are not sufficiently secured, series of comprehensive measures to promote a more effective protection of the sphere, should

follow. Recommended management practices of key areas are outlined schematically. Their detailed analysis would have been beyond this article. This method should be useful especially for small and medium-sized businesses.

## References


**AMERICAN NATIONAL STANDARDS INSTITUTE.** Available at: http://www.ansi.org

ANDERSON, R. (2008) Security Engineering: *A Guide to Building Dependable Distributed Systems, Second Edition*. Wiley Publishing, Inc., 2008. ISBN 978-0-479-06852-6.

**ANTLOVÁ, K.** (2008) *Informační a znalostní podpora malých a středních podniků [Information and knowledge support for SMEs].* Hradecké dny, 2008. ISBN 978-80-7041-190-2.

**BRITITSH STANDARDS INSTITUTE.** Available at: http://www.bsi-global.com

**BROTHBY, W. K.** (2008) *Information Security Governance: Guidance for Information Security Managers.* ISACA, 2008. ISBN 978-1-933-284-73-6.

**ČSN ISO/IEC 27002.** (2008) Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací *[Information technologies – Safety methods – Set of procedures concerning the information safety management].* ČNI, 2008.

**DOUCEK, P.; NOVÁK, L.; SVATÁ, V.** (2008) *Řízení bezpečnosti informací [Information safety management].* Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

**EUROPEAN COMMITTEE FOR STANDARDIZATION.**
Available at: http://www.cen.eu

**INFORMATION SYSTEMS AND CONTROL AUDIT ASSOCIATION.**
Available at: http://www.isaca.org

**INTERNATIONAL ORGANIZATION OF STANDARDIZATION.**
Available at: https://www.iso.org

**INTERNATIONAL REGISTER OF ISMS CERTIFICATES.**
Available at: http://www.iso27001certificates.com

**ISO/IEC 27001.** (2005) Information technology – Security techniques – Information security management system.

**ISO/IEC TR 18044.** (2004) Information technology – Security techniques – Information security incident management.

**McAFee.** (2008) Does Size Matter? The Security Challenge of the SMB. McAfee, 2008.

**POŽÁR, J.** (2005) *Informační bezpečnost [Information safety].* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

**ŠEBESTA, V.; ŠTVERKA, V.; STEINER, F.; ŠEBSTOVÁ, M.** (2006) *Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a komentované vydání ISO/IEC 27001: 2005 [Practical experience from the implementation of information safety management under ČSN BS 7799-2:2004, a commented edition ISO/IEC 27001: 2005].* ČNI, 2006. ISBN 80-7283-204-2.


## Contact address / Kontaktní adresa


**Ing. David Král, Ph.D.**
Akademie STING, Brno
(kral@sting.cz)