Severity Assessment of Security Incidents

Lukas Kralik, Petr Stipek, Roman Senkerik, Roman Jasek
Department of Artificial Intelligence and Informatics
Faculty of Applied Informatics, Tomas Bata University in Zlin
Zlin, Czech Republic
{kralik, stipek, senkerik, jasek}@fai.utb.cz

Abstract—**This paper demonstrates the possible utilization of multi-criteria decision making methods as a different approach to a severity assessment of security incidents. This may support incident management and help with faster decisions. The demonstrated example is based on the Fuller's method. This method helps with determination of criteria weights that are utilized for an overall evaluation and prioritization of security incidents. The main objective was to propose a very simple and fast method that will be suitable for small and medium companies.**

Keywords-severity assessment; security; incident; incident management; security management, multi-criterial decision making; MCDM.

I. INTRODUCTION

An issue of security incidents and their resolving is inseparably connected with the field of Information and Communication Technologies (ICT). It is necessary to look for more and more effective ways to prevent security incidents due to the increasing heterogeneity, complexity and pressure of confidentiality, integrity, availability or non-repudiation. Each security incident is bound with time pressure, which requires automated and clearly defined steps. One of these steps is a severity assessment of a security incident. It is absolutely necessary since it strongly affects the whole investigation process of the occurred incident.

This paper demonstrates the possibilities of utilization of Multi-Criteria Decision Making methods (MCDM) to assess the severity of the security incidents. This may serve as a basis for the new approach to severity assessment of security incidents.

The main objective of current research is to use the simplest MCDM methods to assess the severity. The process described in Section IV of this paper only demonstrates possible utilizations of MCDM. Values for criteria weights may vary for each company. Also, it is important to mention that this method is intended as a support for already implemented incident management tools and for small and medium companies.

The paper is divided into three parts. The first part is focused on basic terms and necessary theory which introduce readers into issues of security incidents. The following part describes solutions for security incidents and used methods with multi-criteria evaluation. And the final part is about the severity assessment of security incidents. This may help security managers in companies with prioritization of security incidents and their solution.

A. Security incident – basic terms

A security incident is an event in the information system, which causes disruption of confidentiality, integrity, availability or non-repudiation of information due to the failure of security measures or violation of security policy [1]-[5].

A suspected violation of a security policy or an attempt to overcome security measures is very often regarded as a security incident. A security incident usually has the following course: Incident Detection - Analysis of the Incident - Response to the Incident. Detection may be either automatic, based on the information from some monitoring system, or manual, i.e., the incident is reported by someone. The company, which wants to deal with the security incidents and effectively solve them, should have an appropriate security standard and also it must properly present such standard to employees. The next step is the formation of a team, which will be responsible for receiving reports, evidence and solving of incidents, etc. In many cases, this team is called Information Security Incident Response Team (ISIRT). The number of ISIRT members depends on the total number and frequency of security incidents and, of course, on the size of the company. For a proper function, ISIRT must have an adequate equipment, means and mainly authority [5]-[13].

The question is than as to how to determine the severity of the incident. There are many possible ways and approaches. The severity of the incident can be determined based on the value of an impact. In other words, the incident has a financial or a non-financial impact to the company. Another solution is to determine the severity of the incident according to the number and expertise of people who have to deal with the incident (more details are given in Section III). It can be assumed that a different number of people or teams with diverse levels of knowledge will participate in finding solution of various incidents [7]-[9][11]-[13].

1) Security standard

Each security standard must contain three basic elements. The first one is a definition of the security incident. The

 ISBN: 978-1-61208-493-0

security incident must be clearly and understandably described with appropriate examples. These examples should be placed in the attachment.

The next part of the security standard is information about security incident report. Contact should involve address on the intranet, e-mail, phone and the office or workplace address. It is necessary to take into the account that the network infrastructure may not work.

And the last one is a structure of a security incident report - form for reporting incidents [5][9][12][13].

2) Security incident log

Creation of the security incident log is necessary for successful resolving of the particular incident. Information listed in this log includes:

- When the incident has occurred - due to the fact that the incident may be related to other events; it is always advisable to ascertain the exact time.
- Where the incident has occurred - the exact place and its description will enable the investigative team to respond quickly.
- Who committed the incident - the identity of the intruder can sometimes be difficult to identify, but we should try to get about him as much relevant information as possible.
- How the incident has occurred - sometimes we do not have enough information, but we should try to build a probable scenario describing the incident.
- What was the target of an attack - we should also distinguish whether the system was directly attacked or used to preparation for another attack.
- Which security attribute was compromised - integrity, confidentiality, availability and/or non-repudiation.
- What was the nature of the incident – if the incident was intentional or unintentional and if unintentional, thus if there was negligence or lack of knowledge of security policy.
- What measures have been overcome - whether the measures at the physical, logical, organizational, personnel or technical security.
- What asset has impaired - hardware, software (operating system, applications, and databases), network, data, etc.
- What is the probability that the incident will be repeated again - rather low, medium, high or certain [5][9][12][13].

3) Equipment of ISIRT

The team should have developed procedures for dealing with specific types of incidents, and these procedures should be still updated with new types of incidents occurring. Also, they should have prepared a communication plan to make it clear who has to inform whom, or who decides on further action etc.

A basic equipment of this team is a common room (war room), where it will be possible to meet and agree on the next steps in the event of an incident [12][13].

Last but not least, they need access to adequate software and hardware resources - for example, the team will need to make a copy of configuration, logs or possibly an entire partition of the infected system [12][13].

B. Simplified procedure for investigation of an incident

The whole procedure has 7 steps. The biggest problem in practice is in step 3. A top management usually requires immediate recovery of operations, thus there may be no time for ensuring clues and finding causes. However, ignoring this step makes environment/conditions for another step, namely step 6, more difficult. Appropriate measures should be proposed to prevent the recurrence of the incident. Choosing a suitable measure is so difficult, thus the company has no other option than hope that the incident will not occur again [3]. The 7 steps of the procedure are:

1. Identify where a security incident has occurred;
2. As quickly as possible, prevent further damage;
3. Analyze the cause of the security incident and collect clues for further analysis;
4. Remove the cause and restore functionality;
5. Assess damage;
6. Design and implement appropriate measures to prevent a recurrence of this incident;
7. Inform others (employees, top management...) on the results of the investigation [2][6][7].

II. LIFE CYCLE OF SOLUTION OF INCIDENT

To propose a solution of security incidents, we used modified Deming's Plan – Do – Check – Act (PDCA) cycle, which is demonstrated on Figure 1. The life cycle of solution of incidents (security) is composed of 4 parts:

1. Formulation and planning of security incident management;
2. Deployment and operation of security incident management;
3. Evaluation of the incident,
4. Development of security incident management and its improvement [12].

 ISBN: 978-1-61208-493-0

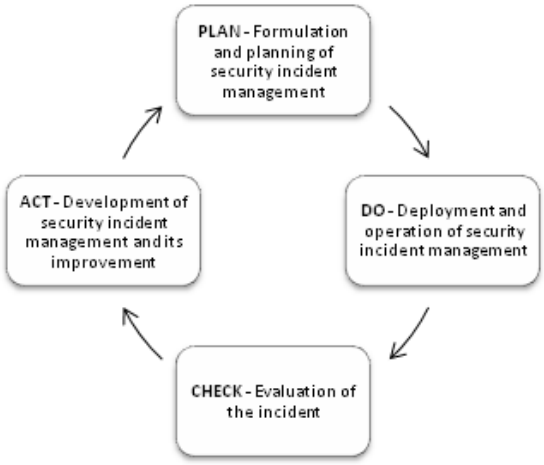

Figure 1. Modified PDCA cycle (adapted from [12])

A. Formulation and Planning of Security Incident Management

Incident Management System, which is based on the organization's security policy, is designed in this phase of the cycle. The main activities in this phase of the life cycle are:

- Preparation and publication policy management of security incidents, including the allocation of the relevant competences and responsibilities.
- Description of the process for reporting security incidents.
- The definition of documents and documentation requirements for employees who are involved in a security incident.
- Verification of the validity of current security documents and documentation management process due to security incidents.
- Building of a team to deal with security incidents, including the determination of competences and obligations within the team and specifying of contact connection.
- Design of crisis scenarios and processes in the event of a crisis state of the organization due to a security incident.
- Plan of staff training in the issue of security incidents and their solving.
- Plans, procedures and methods for testing the process of solving security incidents [8].

B. Deployment and Operation of Security Incident Management

It represents the actual deployment of the entire process into practical use in the company. The following groups of activities are carried out in this phase of the life cycle:

- Event detection;
- Identification, determination, preparation of solutions;
- Solving of security incident.

1) Event detection

This is a key moment for the successful solving of the security incident. The reason is very simple. In this phase, the user of information system encounters the security event. But it is very important that the user is able to recognize and classify the event. Is this event a security incident or not? This is a question which the user must answer. So, it is crucial to spread awareness about the security between users of information system and other employees. The security system will be effective only if employees are able to detect and recognize the incident in time.

Sufficient primary information is another important point for the future solving of the security incident. That is the reason why the essential part of solution is an administrative nature – filling forms, building reports, etc. The basic document is the form for the security event report.

2) Identification, determination and preparation of solutions

The decision is the following step for solving a security incident –is it a security incident which has to be solved by the incident team? This decision is in competence of the security team. The main objectives of the employees to support the security team are:

- Find out as much information as possible about the security event.
- Make primary identification and classification of the incident.
- Make documentation about the information found.
- Inform the security team and, eventually, the incident team [12].

Primary identification of the incident is a significant activity. Important actions during this activity are related to determination and ensuring of:

- Cause of security incident
- Place where security incident occurred
- Way how security incident occurred
- Scope of affected assets [12].

3) Solving of security incident

The incident team should verify and analyze all obtained information very fast and decide if they can solve the incident by internal resources or if they will need help from an external expert. It is essential to make detailed documentation of the whole process of solving of the security incident. This documentation might be used for future solution of identical or similar security incidents [12].

C. Evaluation of the incident

Evaluating the security incident switches security management from the passive role to the active role,

 ISBN: 978-1-61208-493-0

respectively, proactive. The solving of the incident dispels the current complications of the company. Subsequent analysis of the incident should bring benefits to the company to overcome complications. This means lessons from the causes of the incident and subsequently updates of a security risk analysis. On the basis of this fact, risks are revised. The content of the evaluation phase is:

- A more detailed analysis of the incident and its conclusions;
- Updating data about solutions of security incidents;
- Lessons from the incident for the needs to increase security awareness within the company;
- Impact of the incident on the process and content management of security incidents [12].

At the periodical evaluation of security in the company, conclusions resulting from security incidents are used for development and improvement of the security management system [11][12].

D. Development of security incident management and its improvement

In this phase, the experiences gained in dealing with security incidents are included into the security management system of the entire organization. The main aim of this phase is to generalize obtained knowledge from the security incident. The prime activities are:

- Generalize conclusions from the security incident towards risk analysis, its implementation and management.
- Generalize impacts of the incident on Security Management - update the security documentation, etc.
- Identify and implement any changes to the Security Management System [12].

This last phase represents the final feedback, when the experience, skills and knowledge gained during the solving of the security incident reflects into the strategic level of Security Management and Security Policy of the company.

III. ASSESSMENT OF SEVERITY OF INCIDENT

It is very often a problem to correctly determine the severity of the incident. In addition, the severity may vary throughout the life cycle of the incident. For example, at the beginning of the investigation of the incident, it may seem that this is a security incident with a negligible impact on the company and later, during the investigation, it may prove that the original assumption was wrong [11]-[13].

If companies already have established the process that could be used with some exaggeration as an incident management and the severity of each incident is determined in this process, then their approach is very different [12] [13]. It is understandable that different companies use various number of degrees to reflect the severity of the incident and also individual levels have other names [7][11]. However, it is striking that for determining the degree of severity, the companies do not have defined clear rules [13].

If a company conducted a risk analysis, then it can be relatively easy to determine the severity of the incident based on the value of the asset which confidentiality, integrity or availability has been or may be compromised [11][12]. The proposal of criteria for determining the severity of the incident follows:

The severity should be defined by 4 levels:

- low (1 point)
- middle (2 points)
- high (3 points)
- critical (4 points)

Depending on the amount of affected users:

- one or few users (1)
- whole department (2)
- whole branch (3)
- whole company (4)

According to the level that will deal with the incident:

- technical (IT) support (1)
- lower management (2)
- middle management (3)
- top management (4)

Who should be familiar with the incident:

- one or a few employees of the company (1)
- all employees (2)
- own employees and persons outside the company (3)
- own employees and the public(4)

By level of expertise:

- first level of support (1)
- system administrator (2)
- security expert (3)
- security company (4)[13]

There are a lot of security standards and guidelines which define more criteria (e.g. Computer Security Incident Handling Guide from National Institute of Standards and Technology) [1]. With respect to the size and scope of company, these four levels for assessment of the severity of the incident should be enough for most small companies. As it is shown in the following table (Table I.), it is the most selected criteria (selected by more than half of participants) in a survey with around 50 participants.

 ISBN: 978-1-61208-493-0

TABLE I. CRITERIA FOR SEVERITY ASSESMENT

Criterion	Respondents
Depending on the amount of affected users	*41*
According to a level that will deal with the incident	*36*
Who should be familiar with the incident	*30*
By level of expertise	*34*
By value of affected asset	22
Probability of occurrence	8
Affecting of system functionality	11
Time from occurrence to response	15
Incident priority	11
Availability of known solution	5
Probability of recurrence	7

There are many appropriate methods based on MCDM. These methods should be divided into basic (the most simple), advanced and comprehensive (the most difficult). In this case, Fuller's method is recommended because it is very simple and also each company may customize assessment of severity of security incident according to their needs.

A. *Fuller's method*

This is also known as a method of the Fuller's triangle or mainly the pairwise comparison. This method exists in many modifications and it is determined for finding of preferential relations between a pair of criteria. In the simplest modification of this method, the number of preferences is found out with the respect to all other criteria [14][15][17]. This should be done according to Table III. If criterion in a row is more important than a criterion in a column, then number 1 is typed into the cell, otherwise use 0. In agreement with the number of preferences, normalized weights are determined by the following equation [16]

$$v_i = \frac{f_i}{m(m-1)/2} \quad (1)$$

f_i ..... number of preferences of i-th criterion
m ..... number of criteria
$m(m-1)/2$ ..... number of comparisons

The disadvantage is the fact that, when some criterion has 0 preferences, than its weight will be 0. That is a problem because this criterion is not insignificant [15][16].

Also, there is a modification that respects indifference (same significant criteria). In this case, the cell is filled by the number 0.5 [14][17].

B. *Determining of criteria weights*

As mentioned, this assessment is based on the simply pairwise comparison. Also there are 4 criteria which are compared (Table I.):

1. Depending on the amount of affected users;
2. According to a level that will deal with the incident;
3. Who should be familiar with the incident;
4. By level of expertise.

TABLE II. PAIRWISE COMPARISON

Pair of criteria	Preference		
	first	same	second
1 – 2	4	10	5
1 – 3	1	3	15
1 – 4	5	9	5
2 – 3	4	4	11
2 – 4	6	7	6
3 – 4	2	12	5

Comparison was made on the base of interviews with security managers from security agencies and industry companies (Table II.). Following comparison (Table III.) is a median of selected preferences by participants. Nevertheless, it is important to realize that these values may vary. Every company may have a different opinion on the importance of an individual criterion and simultaneously, they should prefer totally different criteria.

TABLE III. PAIRWISE COMPARISON

	1	**2**	**3**	**4**
1	X	0,5	0	0,5
2	0,5	X	0	0,5
3	1	1	X	0,5
4	0,5	0,5	0,5	X

With the utilization of equation 1, final criteria weights are listed in Table IV. These weights will be used for an overall evaluation and severity assessment according to equation 2.

TABLE IV. CRITERIA WEIGHTS

Criterion	Weight [-]
Depending on the amount of affected users	0.167
According to a level that will deal with the incident	0.167
Who should be familiar with the incident	0.417
By level of expertise	0.250

C. *Severity assessment*

Every criterion has a scale with 4 values corresponding to the severity level for each criterion. The overall severity is normalized and expressed as a dimensionless number:

$$S = \sum_{i=1}^{n} C_i \cdot W_i \quad (2)$$

S ..... Severity
C_i ..... Value of the i-th criterion
W_i ..... Weight of the i-th criterion

In practice, most incidents are not so important or dangerous for system stability [6][8][10]. This may cause difficult prioritization of individual incidents. Simple and small modifications in proposed process should make this

 ISBN: 978-1-61208-493-0

prioritization better. The mentioned modification is in scale for each criterion and also companies may propose their own criteria with utilization of this proposed assessment.

The main benefit of the proposed procedure is in speed and simplicity. These two factors are the most important for small companies. Also, this procedure may extend existing incident management in medium companies and provide faster decision making.

IV. Conclusion and Future Work

Security incidents and their solutions are an essential part of life of IS/ICT managers, as well as of ordinary users. Absolute security of an information system is not guaranteed by implementation of any security policy. Although the implementation of various security functions and measures are part of ensuring security, vulnerabilities remain in the information system and these vulnerabilities represent risks. The existence of these vulnerabilities is the possibility of the security incident with direct or indirect impact on everyday operations of companies. Therefore, it is essential that each company pay attention to the definition and the implementation of security management system, its control and audit. At the same time, companies should also deal with efficient and professional management of security incidents. Incidents can be controlled intuitively or in a structured way - professionally. Only a professional approach allows gaining benefits from security incidents - experience, skills and knowledge from solutions of previous security incidents.

The next step in this research is extending the set of criteria which will focus on different aspects (financial and technical/technological impact). The method for the determining of criteria weights will be change for more comprehensive and sophisticated based on intelligent systems (probably fuzzy approach). The main goal for future work and research is a development of continual severity assessment procedure. The final work will be compared with existing assessment methods and also it will be tested in practice.

Acknowledgment

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Programme project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089 and also by the Internal Grant Agency of Tomas Bata University under the project No. IGA/CebiaTech/2016/006.

References

[1] NIST, “Special Publication 800-61 – Computer Security Incident Handling Guide, Revision 2: 800-861“, 2012.

[2] International Organization for Standardization ISO/IEC 27000-Information technology-Security techniques-Information security management systems-Overview and vocabulary.

[3] International Organization for Standardization ISO/IEC TR 18044:2004- Information technology - Security techniques - Information security incident management.

[4] International Organization for Standardization ISO/IEC 27001 - Technology-Security Techniques - Information Security Management Systems-Requirements.

[5] Czech. Act nr. 181/2014 sb. Cyber Security Act. 2014.

[6] P. Doucek “IS/ICT Security Incidents and theire Solutions,” System Integration vol. 3, Prague 2005, pp. 77-85.

[7] L. Wan-Soo and J. Sang-Soo, “A Study on Information Management Model for Small and Medium Enterprises,” Recent Advances in E-Activities, Information Security and Privacy, Spain, WSEAS Press, 2009, pp. 84-87 ISSN: 1790-5117. ISBN: 978-960-474-143-4.

[8] K. Prislan and I. Bernik, “Risk Management with ISO 27000 Standards in Information Security,” In Advances in E-Activities, Information Security and Privacy, Venezuela WSEAS Press 2010, pp. 58-63 ISBN: 978-960-474-258-5.

[9] L. Kralik and R. Senkerik, “Proposal for Security Management System,” Recent Advances in Electrical Engineering and Educational Technologies. Proceedings of the 2nd International Conference on Systems, Control and Informatics (SCI 2014), Athens, 2014. p. 77-80. ISBN 978-1-61804-254-5.

[10] S. Fenz and A. Ekelhart, “Formalizing Information Security Knowledge," 4th International Symposium on Information, Computer, and Communications Security, ACM, 2009, pp. 183-194, 10.1145/1533057.1533084.

[11] L. Kralik, R. Senkerik, and R. Jasek, “Different Aproaches to Security Incidents and Proposal of Severity Assessment of Security Incident,” The Ninth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2015), IARIA, Aug. 2015, pp. 185-189, ISBN: 978-1-61208-427-5.

[12] L. Kralik, R. Senkerik, and R. Jasek, “Model for comprehensive approach to security management,” International Journal of System Assurance Engineering and Management, vol. 7, pp. 129-137, Jun. 2016, doi: 10.1007/s13198-016-0420-8.

[13] L. Kralik, R. Senkerik and R. Jasek, "Integrated security system management and incident management from the perspective of organizational structure," International Conference on Logistics, Informatics and Service Sciences (LISS 2015), IEEE, Jul. 2015, pp. 1-6, doi: 10.1109/LISS.2015.7369766.

[14] M. Cerny and D. Gluckaufova. “Multicriterial evaluation in practice”, Statni nakladatelstvi technicke literatury, 1982.

[15] J. Fotr and L. Svecova, “Managerial decisions: processes, methods and tools,” Ekopress, 2010. ISBN 978-80-86929-59-0.

[16] J. Krupka, M. Kasparova, and R. Machova, “Decision Processes,” University of Pardubice, 2012, ISBN 978-80-7395-478-9.

[17] W. Ho, X. Xu, and P. K. Dey, “Multi-criteria decision making approaches for supplier evaluation and selection: A literature review,” European Journal of Operational Research, Elsevier, 2010, pp. 16-24, ISSN: 0377-2217.

 ISBN: 978-1-61208-493-0