Motivation-Based Risk Analysis Process for IT Systems

Agata Niescieruk, Bogdan Ksiezopolski

Motivation-based risk analysis process for IT Systems

Agata Niescieruk[1] Bogdan Ksiezopolski[1,2]

[1] Polish-Japanese Institute of Information Technology
Koszykowa 86, 02-008 Warsaw, Poland.
[2] Institute of Computer Science, Maria Curie-Sklodowska University,
pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland.

Abstract. Information security management is one of the most important issues to be resolved. The key element of this process is risk analysis. The standards are (ISO/IEC 27000, ISO/IEC 31000) based on the complex and time consuming process of defining vulnerabilities and threats for all organisation assets. In the article we present a new approach to analysing the risk of an attack on information systems. We focus on human factor - motivation, and show its relation to hacker profiles, as well as impacts. At the beginning we introduce a new model of motivation-based risk analysis. Then we describe case study illustrating our approach for a simple set of organisation processes.

1 Introduction

The ISO/IEC 27001 standard, as the part of the growing ISO/IEC 27000 family of standards, brings information security under explicit management control. Being a formal specification, ISO/IEC 27001 provides requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System. ISO/IEC 27001 requires a systematic examination of information security risks, taking into account threats, vulnerabilities, and impacts, designing and implementing a coherent and comprehensive suite of information security controls to address those risks, as well as adopting an overarching management process to ensure that the information security controls continue to meet the information security needs. Information security risks can be estimated according to the different approaches which can be categorised as the quality or quantity analyses, with deterministic or probabilistic methods. However, the most common methods (FRAP, STIR, CRAMM, CORAS, STIR - [10, 13]) consist of the same three stages - risk identification, risk estimation and risk prioritization. All these methodologies have two significant limitations. The first is that while estimating the probability of an attack [12] the methods focus on vulnerabilities [3], threats, weaknesses of resources only in one dimension, treating elements as independent. The second limitation is that motivation as a human factor is neglected. The literature on the subject contains only brief discussions of motivation as a factor influencing risk [9, 1, 2, 11].

The main contribution of the paper is introducing a new motivation-based risk analysis process which focuses on human motivation as the main factor which determines the decision of the attack on an IT system. Another contribution, as opposed to traditional risk analysis, which study individual assets in isolation, is that our method is multidimensional. We try to combine processes and assets involved in them.

2 The Model

In the article we propose a new model for motivation-based risk analysis process. Our modified model is presented in the figure 1. In the following sections all steps are described.

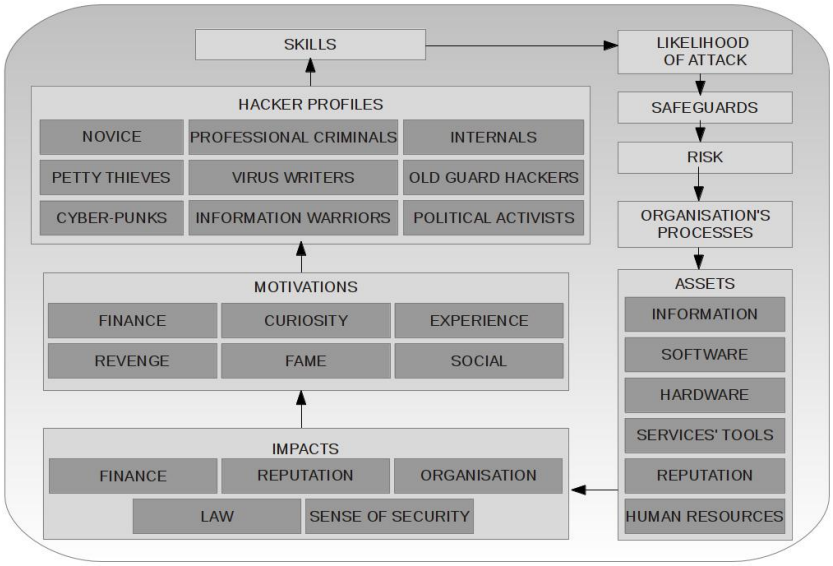

Fig. 1. The model of motivation-based risk analysis process

2.1 Step 1 - Organisation's processes

In the first step we have to focus on all processes in the organisation. They are crucial in realisation of business objectives and require many different resources. In this step we create a set of processes for which the risk will be estimated: $P_1, ..P_n$.

2.2 Step 2 - Assets

In the second step we have to enumerate all assets which take part in the processes defined in the first step. All assets we will denote by A. Referring to ISO 27002 we have 6 groups of our assets, so $A = \{I, S, H, T, R, P\}$, where

1. $I = \{I_1, ..., I_n\}$ - information;
2. $S = \{S_1, ..., S_n\}$ - software;
3. $H = \{H_1, ..., H_n\}$ - hardware;
4. $T = \{T_1, ..., T_n\}$ - services' tools;
5. $R = \{R_1, ..., R_n\}$ - non-material assets - reputation;
6. $HR = \{HR_1, ..., HR_n\}$ - human resources.

For each type of processes n the number of assets can be different. Now for chosen processes we should identify their assets. We will ascribe assets for process P_j as A_j. All assets influence the performance and the development of a company. Each single asset is involved in at least one process, each process uses at least one asset.

2.3 Step 3 - Impact

Undisturbed work of each process is crucial to an organisation and has certain influence. We would like to introduce process impacts as a method of distinguishing between processes. We expect these impacts belong to at least one of these groups:

- finance (higher costs, lower profits, shares depreciation) $[fin]$;
- reputation (violation of trust, damage to brand reputation) $[rep]$;
- organisation (redundancies, lowered morale) $[org]$;
- law (legal obligations, leakage of personal data) $[law]$;
- sense of security (loss of control, awareness of a threat) $[sec]$.

Therefore each single asset a is represented as a vector of impacts:

$$imp_a = [fin_a, rep_a, org_a, law_a, sec_a]$$

where individual elements correspond to the list above and each of them has values from [0..1] with 0 meaning none and 1 meaning the highest possible impact. Similarly for each process P_j, we have a vector of impacts:

$$imp_{P_j} = [fin_{P_j}, rep_{P_j}, org_{P_j}, law_{P_j}, sec_{P_j}]$$

Now we can calculate total impacts for each process and all its assets. Having process P_j and a set of all its assets A_j, the total impacts will be:

$$imp_{P_j,A_j} = [fin_{P_j,A_j}, rep_{P_j,A_j}, org_{P_j,A_j}, law_{P_j,A_j}, sec_{P_j,A_j}]$$

where each element of this vector is calculated as follows:

$$x_{P_j,A_j} = x_{P_j} \cdot [max_{a \in A_j} + (1 - max_{a \in A_j}) \cdot (median_{A_j \setminus max_{a \in A_j}})],$$

where: $x \in \{fin, rep, org, law, sec\}$. The reason why we take the maximum and add it to the median multiplied by 1 - maximum is the fact that we want to have total impacts as numbers from [0..1].

2.4 Step 4 - Motivation

Different impacts for the assets determine certain types of motivation. These categories of motivation [8, 1] that are related to attack on IT system could be one or combination of more of these listed below:

- finance [$finm$];
- curiosity [cur];
- experience/knowledge [exp];
- revenge/anger [rev];
- fame/notoriety [fam];
- social - membership of group (e.g. radical beliefs, political activists) or a desire to impress a group [soc].

The impacts and the motivations are strongly related. In [11] they are parts of sequential steps. However, we did not find this relation directly described in the literature. That is why we introduce 5 levels to describe it: 1 - very high, 0.75 - high, 0.5 - medium, 0.3 - low, 0.1 - very low. For each type of motivation various impacts have various meanings. Using levels above, the relation is illustrated by matrix:

$$mot_{imp} = \begin{bmatrix} finm_{fin} & finm_{rep} & finm_{org} & finm_{law} & finm_{sec} \\ cur_{fin} & cur_{rep} & cur_{org} & cur_{law} & cur_{sec} \\ exp_{fin} & exp_{rep} & exp_{org} & exp_{law} & exp_{sec} \\ rev_{fin} & rev_{rep} & rev_{org} & rev_{law} & rev_{sec} \\ fam_{fin} & fam_{rep} & fam_{org} & fam_{law} & fam_{sec} \\ soc_{fin} & soc_{rep} & soc_{org} & soc_{law} & soc_{sec} \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0.5 & 0.3 & 0.5 & 0.3 \\ 0.3 & 0.75 & 0.5 & 0.1 & 0.75 \\ 0.1 & 0.5 & 0.75 & 0.3 & 0.75 \\ 0.75 & 0.75 & 0.1 & 0.5 & 0.3 \\ 0.5 & 0.75 & 0.5 & 0.5 & 0.5 \\ 0.5 & 1 & 0.5 & 0.3 & 0.3 \end{bmatrix}$$

Each element of this matrix bind a certain type of motivation with a certain type of impact, i.e. for whichever x_y, x is a kind of motivation, y - type of an impact. E.g. fam_{org} is about fame motivation and organisation impact. To obtain exact values, the proper motivations for our process are:

$$mot_{P_j} = [finm_{P_j}, cur_{P_j}, exp_{P_j}, rev_{P_j}, fam_{P_j}, soc_{P_j}]$$

where each element of this vector is calculated in a similar way, e.g.:

$$finm_{P_j} = max(fin_{P_j,A_j} \cdot finm_{fin}, rep_{P_j,A_j} \cdot finm_{rep},$$

$$org_{P_j,A_j} \cdot finm_{org}, law_{P_j,A_j} \cdot finm_{law}, sec_{P_j,A_j} \cdot finm_{sec})$$

2.5 Step 5 - Hacker profile

The next component of our model is a hacker profile. It is determined by his or her motivation [4]. According to article [8] we define the taxonomy of hackers. There are nine primary categories of hackers: Novices [No], Cyber-punks [CP], Internals [In], Petty Thieves [PT], Virus Writers [VW], Old Guard hackers [OG], Professional Criminals [PC], Information Warriors [IW] and Political Activists [PA]. We have to link these hacker profiles with motivation. Referring to the categories of motivation above and to the hacker profiles [8] we define the relationship between them which are presented in the tab. 1.

Table 1. The combination of hacker profile with motivation

	Motivation					
Hacker profile	$finm$	cur	exp	rev	fam	soc
No	no	no	yes	no	no	yes
CP	yes	no	no	no	yes	no
In	yes	no	no	yes	no	no
PT	yes	no	no	yes	no	no
VW	no	yes	no	yes	no	no
OG	no	yes	yes	no	no	no
PC	yes	no	no	no	no	no
IW	yes	no	no	no	no	yes
PA	no	no	no	no	yes	yes

In this step, having calculated values for all types of motivation for a chosen process j we will be able to determine hacker profile. Basing on [8] and [1] we propose matrix which will be used to represent levels of motivation for all types of hackers.

$$mot_{hac} = \begin{bmatrix} 0 & 0.5 & 0.3 & 0.7 & 0 & 0 & 1 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 0.7 & 0.3 & 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 \\ 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \end{bmatrix}$$

Each column corresponds to a hacker profile (first to No, second to CP, etc.) and each row is for a different type of motivation ($finm, cur, exp, rev, fam, soc$). E.g. $mot_{hac}[1,1] = finm_{No} = 0$ is finance motivation for Novices, $mot_{hac}[4,4] = rev_{PT} = 0.3$ is revenge for Petty Thieves. Now we can multiply a vector of motivations for a process j (mot_{P_j}) by this matrix of hackers (mot_{hac}). As a result we obtain vector which has 9 elements, and each one corresponds to one hacker profile:

$$mot_{P_j,hac} = mot_{P_j} \cdot mot_{hac} =$$
$$= [No_{P_j}, CP_{P_j}, In_{P_j}, PT_{P_j}, VW_{P_j}, OG_{P_j}, PC_{P_j}, IW_{P_j}, PA_{P_j}]$$

2.6 Step 6 - Hackers' skills

We have our processes, assets, impacts, motivation and hacker profiles. However, there is one more crucial factor - hackers' skills. Each group of hackers is at a certain level of knowledge and we need to include that factor to our analysis. According to [8] the least skilled group are No, the next are CP and PT, then In, VW, and the most skilled are OG, PC, IW and PA. We define the skills vector as:

$$skl_{hac} = [skl_{No}, skl_{CP}, skl_{In}, skl_{PT}, skl_{VW}, skl_{OG}, skl_{PC}, skl_{IW}, skl_{PA}] =$$

$$= [0.2, 04, 0.6, 0.4, 0.8, 1, 1, 1, 1]$$

2.7 Step 7 - Likelihood of attack

Having a vector of hacker profiles and a vector of their skills we could now estimate which groups of hackers are highly probable to attack. We estimate it by the following multiplication.

$$att_{P_j} = mot_{P_j,hac} \cdot skl_{hac} =$$

$$= [att_{No,P_j}, att_{CP,P_j}, att_{In,P_j}, att_{PT,P_j},$$

$$att_{VW,P_j}, att_{OG,P_j}, att_{PC,P_j}, att_{IW,P_j}, att_{PA,P_j}]$$

All elements of this result vector are from [0..1]. For a number less than 0.1 we will talk about a small likelihood of an attack, for numbers from [0.1..0.5] the likelihood will be at a medium level. Finally, values greater than 0.5 will mean the likelihood is high. Our method has just showed whether the process is critical and could be interesting for a hacker of a certain type - the likelihood of an attack. The question whether this attack will be successful or not could not be answered here as we did not analyse safeguards.

2.8 Step 8 - Safeguards

In the next step the safeguards for all analysed processes must be defined. We suggest using a scale: 1 - very high, 0.75 - high, 0.5 - medium, 0.25 - low, 0 - very low. That means, if there is a level 1, the safeguards are strong, so the assets are properly protected. At the same time, level 0 means that the assets are practically unsecured. We will denote the safeguard level as SF, and it is a number used for all assets taking part in the specific process. However the analysis could be extended to a version where we identify separate safeguard levels for each asset.

2.9 Step 9 - Risk

Finally, the risk of specific processes can be calculated - $Risk_{P_j}$ (Risk for the process j). The risk is estimated by the following formula.

$$Risk_{P_j} = (1 - SF^2)_{P_j} \cdot att_{P_j}$$

In our model the risk can be a value from 0..1 where 0 means no risk and 1 means that it is highly probable that potential attack will be successful. That is why, we multiply the likelihood by $1 - SF^2$. Results greater or equal 0.5 show a very high risk of a successful attack.

3 The Case Study

In the next section we demonstrate our new method for motivation-based risk analysis. Due to the space limitations we are prepare an analysis of a simple example where each component of our model will be described and final risk of an attack will be calculated.

3.1 Step 1 - Processes

In our example we define a small online store. Let $P_1, P_2, P3$ be our crucial processes in this chosen company. P_1 is registration of a new customer (standard form on the website and then an authentication mail sent to an address given), P_2 is a payment for an order (with finished shopping going to a bank webpage), P_3 is viewing archive orders (list of an user's previous orders with prices and products bought). As a result of this step we have a list of defined processes.

3.2 Step 2 - Assets

According to our model, now we have to present assets. There are many of them in this company, but those that are relevant to our processes are:

- I_1 (databases with personal data, orders, and products data);
- S_1 (web server), S_2 (mail authentication app.), S_3 (api to bank payments);
- H_1 (server), H_2 (router);
- T_1 (air conditioning), T_2 (power).
- R_1 (good reputation);
- HR_1 (administrator).

In process P_1 we have all assets except S_3, in P_2 all assets except S_2, in P_3 all assets except S_2 and S_3. Therefore:

$$A_1 = \{I_1, S_I, S_2, H_1, H_2, T_1, T_2, R_1, HR_1\}$$

$$A_2 = \{I_1, S_I, S_3, H_1, H_2, T_1, T_2, R_1, HR_1\}$$

$$A_3 = \{I_1, S_I, H_1, H_2, T_1, T_2, R_1, HR_1\}$$

3.3 Step 3 - Impact

Having processes and assets, we should define impacts for all of them. As it was presented in section 2.3, below we combine impacts with assets:

$$imp_{I_1} = [0.6, 0.5, 0.4, 0.4, 0.5], imp_{S_1} = [0.3, 0.8, 0.6, 0.5, 0.5],$$

$$imp_{S_2} = [0.1, 0.5, 0.7, 0.7, 0.4], imp_{S_3} = [1, 0.6, 0.5, 0.8, 1],$$

$$imp_{H_1} = [0.6, 0.5, 0.7, 0.4, 0.6], imp_{H_2} = [0.5, 0.5, 0.4, 0.3, 1],$$

$$imp_{T_1} = [0.6, 0.4, 0.75, 0.1, 0.4], imp_{T_2} = [0.6, 0.75, 0.6, 0.3, 0.4],$$

$$imp_{R_1} = [0.75, 1, 0.4, 0.4, 0.4], imp_{HR_1} = [0.5, 0.4, 0.75, 0.5, 0.75].$$

Similarly, impacts for processes are:

$$imp_{P_1} = [0.5, 0.8, 0.9, 0.4, 0.8], imp_{P_2} = [1, 0.7, 0.4, 0.5, 0.9],$$

$$imp_{P_3} = [0.3, 0.6, 0.3, 0.6, 0.5].$$

Next, we calculate vectors of total impacts for the three processes.

$$imp_{P_1,A_1} = [0.44375, 0.8, 0.81, 0.328, 0.8]$$

$$imp_{P_2,A_2} = [1, 0.7, 0.355, 0.44, 0.9]$$

$$imp_{P_3,A_3} = [0.27, 0.6, 0.27, 0.42, 0.5]$$

3.4 Step 4 - Motivation

The following step is to calculate vectors of motivation for each process. We do that by taking the maximum of the products from multiplying elements of mot_{imp} - matrix with $1, 0.75, 0.5, 0.3$ and 0.1 by already calculated elements of the impact vector, for each process imp_{P_i,A_i}.

$$mot_{P_1} = [0.44375, 0.6, 0.6075, 0.6, 0.6, 0.8]$$

$$mot_{P_2} = [1, 0.675, 0.675, 0.75, 0.525, 0.7]$$

$$mot_{P_3} = [0.3, 0.45, 0.375, 0.45, 0.45, 0.6]$$

3.5 Step 5 - Hacker profile

Now we can multiply motivation vectors by hacker profile matrix (mot_{hac}) and we obtain three vectors that correspond to hacker profiles.

$$mot_{P_1,hac} = [0.7, 0.52, 0.55, 0.49, 0.6, 0.6, 0.44, 0.62, 0.7]$$

$$mot_{P_2,hac} = [0.69, 0.76, 0.82, 0.92, 0.71, 0.68, 1, 0.85, 0.61]$$

$$mot_{P_3,hac} = [0.49, 0.38, 0.40, 0.34, 0.45, 0.41, 0.30, 0.45, 0.52]$$

3.6 Step 6 - Hackers skills

As we defined before, the skills vector is as follows:

$$skl_{hac} = [0.2, 04, 0.6, 0.4, 0.8, 1, 1, 1, 1],$$

where consecutive values correspond to No, CP, In, PT, VW, OG, PC, IW, PA.

3.7 Step 7 - Likelihood of attack

Finally we will calculate the likelihood of an attack - multiplying $mot_{P_j,hac}$ by skl_{hac}:

$$att_{P_1} = [0.14, 0.208, 0.33, 0.196, 0.48, 0.6, 0.44, 0.62, 0.7]$$

$$att_{P_2} = [0.138, 0.304, 0.492, 0.368, 0.568, 0.68, 1, 0.85, 0.61]$$

$$att_{P_3} = [0.098, 0.152, 0.24, 0.136, 0.36, 0.41, 0.3, 0.45, 0.52]$$

All values are in range [0..1]. However the highest value is for process P_2 - we see that $att_{PC,P_2} = 1$. We may conclude that this process is alluring for Professional Criminals, which does not seem to be astonishing. What is also worth mentioning is that P_3 is safe, only the last value is for medium likelihood, but it is low.

3.8 Step 8 - Safeguards

The safeguards are in our method for all assets, so let our company be in the middle of a scale with $SF = 0.5$. That means there is some security but it could be not sufficient enough.

3.9 Step 9 - Risk

To obtain risk, we now calculate the likelihood of an attack by $1 - SF^2 = 0.75$. It gives us:

$$Risk_{P_1} = [0.105, 0.156, 0.2475, 0.147, 0.36, 0.45, 0.33, 0.465, 0.525]$$

$$Risk_{P_2} = [0.1035, 0.228, 0.369, 0.276, 0.426, 0.51, 0.75, 0.6375, 0.4575]$$

$$Risk_{P_3} = [0.0735, 0.114, 0.18, 0.102, 0.27, 0.3075, 0.225, 0.3375, 0.39]$$

During the analysis of results one can see that the risk vector for the second process has several values greater than 0.5. It means that there is a high probability of a successful attack on this process and a risk reduction method should be applied.

4 Conclusions

The risks analysis for IT systems is one of the major activities in the information security management. In the article we present motivation-based risk analysis which estimates the risk based on the attack motivation as the human factor. The presented approach is less complicated that the standard one which based on the vulnerabilities and threats analysis. Another feature of the presented approach is that the new method for risk analysis is multidimensional. Owing to that, the calculated risks of the a given process will take into account all assets taking part in the analysed process. In the article we present a case study for our methodology where risks of simple processes were calculated. The proposed risk analysis method can be used as part of Quality of Protection models [6, 7] which introduce adaptable security [5] for IT Systems.

Acknowledgements

This work is supported by Polish National Science Centre grant 2012/05/B/ST6/03364

References

1. R. Barber: Hackers Profiled - Who Are They and What Are Their Motivations?: Computer Fraud & Security, 2, 1, pp. 14-17(4), 2001.
2. J. Gao, B. Zhang, X. Chen, Z. Luo: Ontology-Based Model of Network and Computer Attacks for Security Assessment. Journal of Shanghai Jiaotong University, 18, 5, pp 554-562, 2013.
3. M. Gerber, R. Solms: Management of risk in the information age. Computer & Security, 14, pp. 16-30, 2005.
4. L. Grunske, D. Juoyce: Quantitative risk-based security prediction for component-based systems with explicity modeled attack profiles. Journal of Systems and Software 81, 8, pp. 13271345, 2008.
5. B. Ksiezopolski B, Z. Kotulski: Adaptable security mechanism for the dynamic environments. Computers & Security; 26, pp.246-255, 2007.
6. B. Ksiezopolski, QoP-ML: Quality of Protection modelling language for cryptographic protocols . Computers & Security; 31(4), pp.569-596, 2012.
7. B. Ksiezopolski, D. Rusinek, A. Wierzbicki: On the efficiency modelling of cryptographic protocols by means of the Quality of Protection Modelling Language (QoP-ML). LNCS, 7804, pp.261-270, 2013.
8. M. K. Rogers: A two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigation, 3, 2, pp. 97102, 2006.
9. M. K. Rogers, K. Seigfried, K. Tidke: Self-reported computer criminal behavior: A psychological analysis: Digital Investigation 3, pp. 116120, 2006.
10. L. Othmane, H. Weffers, M. Klabbers: Using Attacker Capabilities and Motivations in Estimating Security Risk. SOUPS, 2013.
11. NIST SP 800-30: Risk Management Guide for IT Systems, 2008.
12. O. Sheyner, J.Haines, S.Jha, R.Lippman, J.M.Wing: Automated generation and analysis of attack graphs. S&Pi, 2002.
13. N. Vavoulas, C. Xenakis: A Quantitative Risk Analysis Approach for Deliberate Threats, CRITIS, pp. 13-25, 2011.