FREQUENTLY-OCCURING SECURITY INCIDENTS

Predrag Tasevski, MSc
Cybersecurity.mk
Kumanovo, Macedonia

ABSTRACT

Risk Assessment is a common part of Risk Management, also, traditionally the focus has always been on the evaluation of the risk in organizations through probability, rather than by the frequency of security incident occurrence. The aim of our work was to further develop the knowledge of risk impact by frequency of any given security incident occurrence.

INTRODUCTION

Risk assessment is a vital step in Risk Management, it aims to determine the quantitative or qualitative value of risks related to an array of threats (i.e. attacks) at any given point in time. Many individuals, organizations, and those they interconnect with will have to be able to identify, prioritize and estimate risks. Additionally, we have to keep in mind that a security incident happens when there are threats, vulnerability, as well as a likelihood for the event will occur.

In general, risk is when the chosen action or activity will lead to organizational loss. In addition, risk is the likelihood that something wrong or/and bad will happen and it will cause harm to the organizational information asset, or lead to the entire loss of the asset. In risk, vulnerability is a weakness that could be used to jeopardize or cause harm. Threat is anything (artificial or act of nature) that has the potential to cause harm to organizational information assets [1].

Moreover, the probability that a threat will use a vulnerability to cause damage creates a risk for the organizations. When a threat uses vulnerability to inflict damage, it has an impact. In the context of information security, the impact is a loss of availability, integrity and confidentiality. Similarly, to information security, in cyber security the additional impacts are: non-repudiation, authentication, information systems importance and criticality from the standpoint of state Critical Information Infrastructure / Critical Infrastructure. Other possible losses can occur too, such as loss of income and loss of life, etc. It is very important to point out that it is impossible to identify all risks, nor is it possible to eliminate all risks.

Therefore, the main goal of this article is to provide background information about information technology related to risks and an illustrated template tool for security risk assessment. Furthermore, it shows how to identify and evaluate the risk elements by delivering a solution with an expanded definition of risks and risk measurement techniques by probability, or even better, by the frequency of security incident occurrence.

BACKGROUND

The first book on computer security appeared in the 1970s, and it was tailored for professionals and the general public. It also served as a public recognition of security as a problem and the value of the risk assessment process. Moreover, the introduction of networked systems had relatively limited impact on the risk profiles of most organisations, since unauthorised access to the network was physically and technically very difficult, and the growth in the numbers of people who entered the computing industry and the incidence of computer crime was also very limited. At this point, the greatest risk was fraud [2], where the most common exploitation techniques involved gaining unauthorised access to an official computer. This is no longer a significant factor nowadays.

Therefore, there have been advances in technology, coupled with the risks and threats they bring along with them, which are startlingly different from the risk landscape of the past. Thus, the scholars and researchers intent to develop novel approaches to increase awareness and define measures necessary to identify, mitigate, prioritize and estimate the risks. Their concentration is mainly on the calculation of risk through the probability of the threats intersecting with vulnerabilities and losses caused by a security incident.

For instance, many organizations – both public and private – nowadays, have implemented and developed their own security risk assessment template tool. The main goal for the template is first to analyse work-flow, then to identify the assets, threat sources and vulnerabilities. Bear in mind that threat sources and the vulnerabilities should be roughly below ten. Otherwise, the combination of threat sources and vulnerabilities may be unmanageable. After having identified threat sources and vulnerabilities for the scope, the next step is the Risk Matrix, illustrated in Figure 1. Here combinations of threat sources and vulnerabilities that match are formally identified. In addition, these threats must be qualified into risks by describing and rating them in terms of likelihood and impact. We specify the risk level, such as, H – High, M – Middle and L – Low risk level. Finally, the risk indicator is identified. For example: smoke, storm warning, server overheating, suspicious behaviour by client or new employees, slow execution of code, website stops working, unexpected results and output, etc.

After the risk matrix, threat sources and vulnerabilities, organizations have to create a mitigation strategy and plan, illustrated in Figure 2. Where the strategy for risk treatment can be:

- Risk Acceptance. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
- Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a

threat's exercising a vulnerability (e.g. use of supporting, preventive, detective controls).

- Risk Transference. To transfer the risk by using other options to compensate for the loss, such as, purchasing insurance.

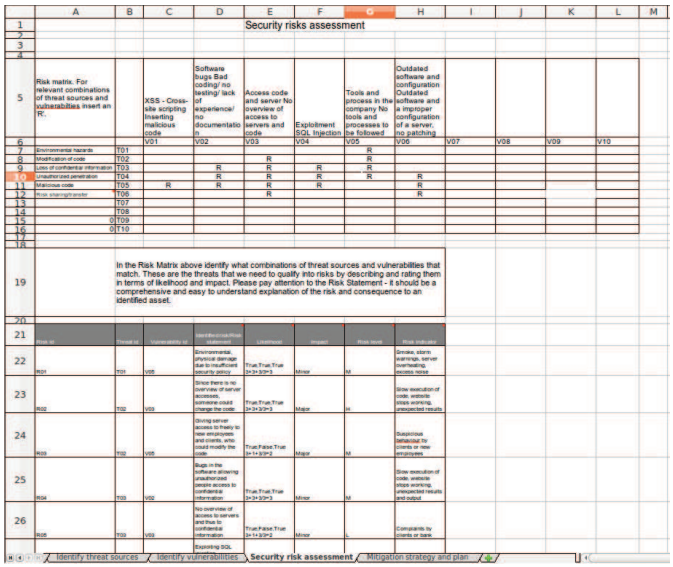

Figure 1: Security Risk Assessment Tool Template.

Further, to specify the risk owner, rationale and risk response, several actions can be required for each risk. Such actions might include mitigations as well as contingency planning. Of course, such a mechanism will want to take into account the planned due date, risk status and status date of each element identified.

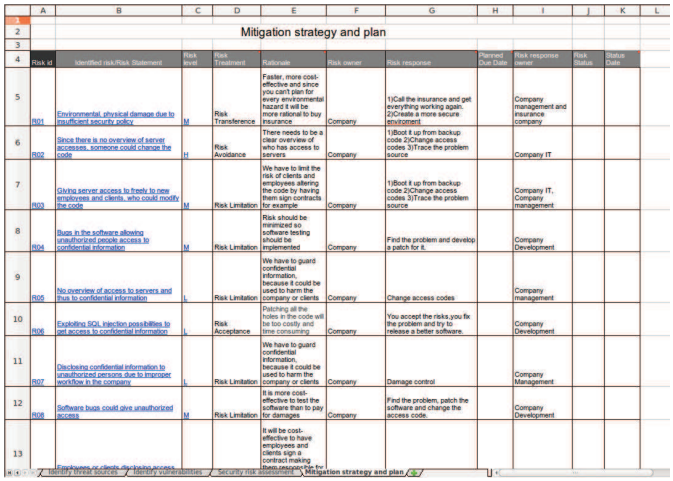

Figure 2: Mitigation strategy and plan matrix.

Nevertheless, this is just a simple template tool that can be extremely useful and beneficial to organizational needs. However, is this enough? For instance, what if the calculated security incident takes place once a year and the Probability=1, but what if the security incident takes place once a month then still the Probability=1, where in reality the sum of losses for organization will be very different. Therefore, in the next methodology section we provide the readers with a simple solution by substituting the probability with a frequency of occurrence, which will provide more useful information to organizations and individuals, and provide for a better and more beneficial measurement of security risk assessment.

METHODOLOGY

As we mentioned previously, Risk Assessment is a single step in Risk Management process, and it is carried out by a team of people who have knowledge of specific areas of the organization. The members of the assessment team may vary over time as different organizational risks are assessed. The assessment may be an intuitive qualitative analysis based on informed opinion, or where reliable cost optimization and historical information is available, the analysis may use quantitative analysis [1]. At the same time, a probability value helps determine the risk by computing losses, but for the organisation's management, this is not the most useful information, especially if the security incident takes place only once a year versus every moth. In this section we provide the reader with a simplified methodological approach of how to calculate and account for frequently-occurring security incidents.

Therefore, we emphasize in this article the Risk Assessment element as a step in the Risk Management procedure to identify, prioritize and estimate risk to an organization's operations, assets, individuals and other interconnected organizations. Where we have to keep in mind that a security incident happens when we have a threat (i.e. attack) and at the same time a vulnerability (i.e. no protective/meditative measures implemented against this concrete attack). For illustration consider [3]:

$$R = P_{robability}(T \cap V) * L \quad ,$$

Where the:

R is risk that could be expressed as the function of the set of threats intersecting with that of vulnerabilities multiplied with loss sustained per incident,

P is defining the probability of: T defines the threats intersect with V – vulnerabilities and

L is the loss caused by a security incident.

However, to be more precise the purpose of the risk assessment element is to identify and evaluate the following:

- Threats for operations, assets, or individuals,
- Vulnerabilities for operations, assets, or individuals,
- Impact for the consequence, losses or opportunity and
- Probability or, even better, Frequency of security incident occurrence.

The reason why it is better to use Frequency is that, for example, in calculating the risks for a year, if the security incident takes place only once a year then Probability=1 but is the security incident takes place more frequently, like once a month then its Probability is still=1, but in reality the sum of losses will be different, i.e. [3]:

$$R = F_{requency}(T \cap V) * L \quad ,$$

This approach and method will help to identify frequently occurring security incidents rather than merely the raw probability of losses. It will aid the organisation is summarizing a clearer picture of losses sustained from the threat/vulnerability. However, this is just a very simple and easy way of estimating and calculating the risk, by identifying the risk that could be a function of threats intersecting with vulnerabilities through losses caused by a security incident.

CONCLUSION

Risk Assessment is neither a simple nor easy process to conduct. It requires certain foreknowledge. Only those who have detailed knowledge of the relevant areas of the organization in question will be able to contribute usefully to the evaluation. Although many organizations and risk management teams posses and are implementing their own security risk assessment template tools, many still cannot derive a useful picture of real losses because they're focusing on the probability or any given risk and ignoring its frequency of occurrence.

Therefore, the main goal of this article is to deliver and emphasize the notion of how to use the frequency of any given security incident's occurrence in order to provide a more useful picture of the risk impact. If the security incident will occur once a year or once a month, the magnitude of loss will be very different. Hence we recommend and stress how to use frequency instead of only probability, when it comes to calculating and measuring security risks.

REFERENCES

[1] Spagnoletti, Paolo; Resca A., "The duality of Information Security Management: fighting against predictable and unpredictable threats," *Journal of Information System Security*, no. 4 (3), pp. 46-62, 2008.

[2] Peter Sommer, Ian Brown, "Reducing Systematic Cybersecurity Risk", *OECD/IFP Project on "Future Global Shocks",* January 2011.

[3] Predrag Tasevski. "Interactive Cyber Security Awareness Program", *LAP Lambert Academic Publishing*, pp. 22-26, August 2012.