electronic periodical
YOUTH SCIENTIFIC AND TECHNICAL BULLETIN
Bauman MSTU Publ EL № FS-77-51038, ISSN 2307-0609

UDC 004.056

INFORMATION SECURITY RISK MANAGEMENT

D.A. Mikov, student
BMSTU, Russia, Moscow, 105005

Scientific supervisor: T.I. Buldakova, doctor of Technical Science,
Professor of Department "Information Security" in BMSTU
Russia, Moscow, 105005
bauman@bmstu.ru

Information security risk is a risk related to information technology. This relatively new term due to an increasing awareness that information security is simply one facet of a multitude of risks that are relevant to IT and the real world processes it supports. Generally speaking, risk is the product of the likelihood of an event occurring and the impact that event would have on an information technology asset [1]. The impact of an event on an information asset is usually taken to be the product of a vulnerability in the asset and the asset's value to its stakeholders. So, the measure of an information security risk (R) can be determined as a product of threat (T), vulnerability (V) and asset (A) values [2]:

$$R = T \times V \times A$$

At the first step of the information security risk management, the external and internal context should be established, which involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organization operating the information security risk management. Depending on the scope and objectives of the risk management, different approaches can be applied. The approach might also be different for each iteration. An appropriate risk management approach should be selected or developed that addresses basic criteria such as: risk evaluation criteria, impact criteria, risk acceptance criteria.

1. Risk evaluation criteria should be developed for evaluating the organization's information security risk considering the followings:

1) the strategic value of the business information process;

2) the criticality of the information assets involved;

3) legal and regulatory requirements, and contractual obligations;

4) operational and business importance of availability, confidentiality and integrity;

5) stakeholders expectations and perceptions, and negative consequences for goodwill and reputation.

Additionally, risk evaluation criteria can be used to specify priorities for risk treatment.

2. Impact criteria should be developed and specified in terms of the degree of damage or costs to the organization caused by an information security event considering the following:

1) level of classification of the impacted information asset;

2) breaches of information security (e.g. loss of confidentiality, integrity and availability);

3) impaired operations (internal or third parties);

4) loss of business and financial value;

5) disruption of plans and deadlines;

6) damage of reputation;

7) breaches of legal, regulatory or contractual requirements.

3. An organization should define its own scales for levels of risk acceptance. The following should be considered during development:

1) risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances;

2) risk acceptance criteria may be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk;

3) different risk acceptance criteria may apply to different classes of risk, e.g. risks that could result in noncompliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement;

4) risk acceptance criteria may include requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period;

5) risk acceptance criteria may differ according to how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity.

Risk acceptance criteria should be set up considering the following: business criteria; legal and regulatory aspects; operations; technology; finance; social and humanitarian factors.

The next step of information security risk management is identification of assets, threats, existing and planned controls, vulnerabilities and consequences.

1. The assets within the established scope should be identified. An asset is anything that has value to the organization and which therefore requires protection. For the identification of assets it should be borne in mind that an information system consists of more than hardware and software.

2. Threats and their sources should be identified. A threat has the potential to harm assets such as information, processes and systems and therefore organizations. Threats may be of natural or human origin, and could be accidental or deliberate. Both accidental and deliberate threat sources should be identified. A threat may arise from within or from outside the organization. Threats should be identified generically and by type (e.g. unauthorized actions, physical damage, technical failures) and then where appropriate individual threats within the generic class identified.

3. Existing and planned controls should be identified. Identification of existing controls should be made to avoid unnecessary work or cost, e.g. in the duplication of controls. In addition, while identifying the existing controls, a check should be made to ensure that the controls are working correctly – a reference to already existing ISMS (Information Security Management System) audit reports should limit the time expended in this task. If a control does not work as expected, this may cause vulnerabilities. Consideration should be given to the situation where a selected control (or strategy) fails in operation and therefore complementary controls are required to address the identified risk effectively. In an ISMS, this is supported by the measurement of control effectiveness. A way to estimate the effect of the control is to see how it reduces the threat likelihood and ease of exploiting the vulnerability, or impact of the incident.

4. Vulnerabilities that can be exploited by threats to cause harm to assets or to the organization should be identified. Vulnerabilities may be identified in following areas: organization; processes and procedures; management routines; personnel; physical environment; information system configuration; hardware, software or communications equipment; dependence on external parties.

5. The consequences that losses of confidentiality, integrity and availability may have on the assets should be identified. A consequence can be loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc. This activity identifies the damage or consequences to the organization that could be caused by an incident scenario. An incident scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities in an information security incident. The impact of the incident scenarios is to be determined considering impact criteria defined during the context establishment activity. It may affect one or more assets or part of an asset. Thus assets may have assigned values both for their financial cost and because of the business consequences if they are damaged or compromised. Consequences may be

of a temporary nature or may be permanent as in the case of the destruction of an asset. Organizations should identify the operational consequences of incident scenarios in terms of (but not limited to): investigation and repair time; (work)time lost; opportunity lost; health and safety; financial cost of specific skills to repair the damage; image reputation and goodwill.

After the identification of basic risk criteria and principal elements of ISMS, risk should be measured.

Information security risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence [3].

OWASP (Open Web Application Security Project) proposes a practical risk measurement guideline based on [4]:

1. Estimation of Likelihood as a mean between different factors in a 0 to 9 scale:

1) Threat agent factors: skill level; motive; opportunity; size;

2) Vulnerability Factors (the next set of factors are related to the vulnerability involved, the goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited, assume the threat agent selected above): ease of discovery; ease of exploit; awareness; intrusion detection;

2. Estimation of Impact as a mean between different factors in a 0 to 9 scale:

1) Technical Impact Factors (technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability – the goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited): loss of confidentiality; loss of integrity; loss of availability; loss of accountability;

2) Business Impact Factors (the business impact stems from the technical impact, but requires a deep understanding of what is important to the company running the application, in general, you should be aiming to support your risks with business impact, particularly if your audience is executive level, the business risk is what justifies investment in fixing security problems): financial damage; reputation damage; non-compliance; privacy violation.

If the business impact is calculated accurately use it in the following otherwise use the Technical impact:

1) rate likelihood and impact in a LOW, MEDIUM, HIGH scale assuming that less than 3 is LOW, 3 to less than 6 is MEDIUM, and 6 to 9 is HIGH;

2) calculate the risk using the summary table.

Overall Risk Severity

Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

And the final step of information security risk management is information security risk treatment. There are four options available for risk treatment: risk modification, risk retention, risk avoidance and risk sharing.

1. Appropriate and justified controls should be selected to meet the requirements identified by the risk assessment and risk treatment. Selection of risk modification should take account of the risk acceptance criteria as well as legal, regulatory and contractual requirements. This selection should also take account of cost and timeframe for implementation of controls, or technical, environmental and cultural aspects. It is often possible to lower the total cost of ownership of a system with properly selected information security controls.

In general, controls may provide one or more of the following types of protection: correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring and awareness. During control selection it is important to weigh the cost of acquisition, implementation, administration, operation, monitoring, and maintenance of the controls against the value of the assets being protected. Furthermore, the return on investment in terms of risk reduction and potential to exploit new business opportunities afforded by certain controls should be considered. Additionally, consideration should be given to specialized skills that may be needed to define and implement new controls or modify existing ones.

There are many constraints that can affect the selection of controls. Technical constraints such as performance requirements, manageability (operational support requirements) and compatibility issues may hamper the use of certain controls or could induce human error either nullifying the control, giving a false sense of security or even increasing the risk beyond not having the control (e.g. requiring complex passwords without proper training, leading to users writing passwords down). Moreover, it could be the case that a control would affect performance. Managers should try to identify a solution that satisfies performance requirements while guaranteeing sufficient information security. The result of this step is a list of possible controls, with their cost, benefit, and priority of implementation.

2. The decision on retaining the risk without further action should be taken depending on risk evaluation. If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls and the risk can be retained.

3. When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision may be made to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated. For example, for risks caused by nature it may be most cost effective alternative to physically move the information processing facilities to a place where the risk does not exist or is under control.

4. Risk sharing involves a decision to share certain risks with external parties. Risk sharing can create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary. Sharing can be done by insurance that will support the consequences, or by sub-contracting a partner whose role will be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage. It should be noted that it may be possible to share the responsibility to manage risk but it is not normally possible to share the liability of an impact. Customers will usually attribute an adverse impact as being the fault of the organization.

References

1. OHSAS 18001: 2007. Occupational health and safety management systems – Requirements.
2. Caballero, Albert. 2009. Chapter 14. Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 232.
3. ISO/IEC FIDIS 27005: 2008. Information technology – Security techniques – Information security risk management.
4. Open Web Application Security Project risk rating Methodology. URL.https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.