Risk Management in Public Key Infrastructure

Nicușor VATRĂ
The Bucharest Academy of Economic Studies, Romania
E-mail: nicusor.vatra@yahoo.com
Daniel Constantin JIROVEANU
The Bucharest Academy of Economic Studies, Romania
E-mail: daniel.jiroveanu@man.ase.ro

Abstract
Nowadays, it is almost impossible not to hear or read about the risks of using computer systems. Top management is becoming more interested in risk management process and their analysis regarding the use of information technologies within their organization. This is due primarily to the Internet boom and high level of dependence of their business to information systems. Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and obtain assets in mission capability by securing the IT systems and data that help their organization's performances .
In this paper, we present the risk-management processes, the main services offered by the Public Key Infrastructure and security risks that may arise in implementing Public Key Infrastructure.

Keywords: *risk management, public key infrastructure, PKI services, PKI risks.*

JEL classification: M10, M15

Introduction

Business success and failure depend very much on information systems and therefore, any organization policy regarding the identification of vulnerabilities, threats and risks must be proactive.

Risks vary from one organization to another, and we may ask why?

The answer to this question is simple: because every organization is unique and is more or less subject to threats that can turn into risks, these must be identified, analyzed, controlled and mitigated.

Risk:

- The likelihood of incurring losses as a result of achieving certain destructive actions by exploring system vulnerabilities.
- The risk is the possible future event whose occurrence will affect the project objectives in terms of cost, calendar program or technical. [1]
- Risk is the possibility that something to occur and have an impact on your objectives is the chance to either make a gain or a loss. It is measured in terms of likelihood and consequence. [2]

The risk, so to speak, is not any fact, which already happened and disturbs the project progress; it indicates the things you guess possibly happen in the future.

In recent years, system information evolution which is vital to any business is required to be low-cost, and its lead time is also required to be shortened. Likewise, wide-ranging methods and techniques for development must be created, examined and selected. Due to such circumstances, developers may start their work, failing to foresee possible troubles at the stage of project launch. They may also neglect signs of emerging troubles and failing to take appropriate countermeasures may lead to the actual troubles, which could expose the project to crises of exceeding budget, delayed delivery, and poor quality.

In 1990s, the transition to the open system becomes a boom focused in the United States. In Romania, after the bust of bubble economy and the economic stagnation, the cost reduction became the top priority. After 1999, the open system was spread rapidly; because its specialty was to aim the cost reduction by adopting the downsizing and open technology. In such stream, the environment of the system development has been changed dramatically. Before that, main framework system was the main stream for the basic system of the Organization. One computer maker provided from the host computer to the hardware of the terminal computer, or the software from Operating Systems to the applications. According to the spread of the open system, the different vendors provided the servers, computers, Operating Systems or applications. As a result, each component of the system became a black box.

The expand of the open system adjusted the system development and the introduction method of the Organization, adequate to the top priority of the cost reduction referred in the previous page, the information system development had no choice but to do the system development within the limited budget. By the appearance of the new open technology, the system development became hard within the Organization considering the cost and technology. Therefore, outsourcing the development to the outside became popular. As a result, it became difficult to accumulate the know-how of the system development and the project management within the Organization.

On the other hand, the other organization which attempted the system development was forced to respond to the cost reduction and to the new technology, and in the end, they also outsourced its system development to the outside.

By such change of the system development environment, it became hard to hold and manage the entire system development. Due to this, it became also quite tough in preventing the system failure or the occurrence of a crash sooner and specifies the cause of the system failure or accident.

Below such circumstances, project managers are obliged to attain goals with limited resources; they need to achieve goals through project management by anticipating the emergence of risks, planning and implementing appropriate countermeasures to reduce the impact.

1. Risk management process

Risk management is the term given to an understandable and systematized process of identifying, analyzing, treating and monitoring the risks implicated in any activity or process. Risk management is a methodology that assists managers to make best utilization of their available resources.

Risk management practices are broad used in public and the private sectors, covering a wide range of activities or operations. Risk management is now an integral part of business planning. The risk-management process steps are a generic guide for any organization, regardless of the type of business, activity or function.

The basic process steps are [1]:

1. Establish the context;
2. Identify the risks;
3. Analyze the risks;
4. Evaluate the risks;
5. Treat the risks;
6. Monitoring and review;
7. Communication and consultation.

'Risk' is dynamic and subject to constant modification, so the process includes ongoing:

- monitoring and review;
- communication & consultation.

a. **Establish the context**.

Establishing the context for any Risk management assessment is actually important. It needs a comprehensive understanding of the background in which an organization exists and acts. Establishing the context specifies the framework for managing the Risk management process.

b. **Identify the risks**.

Previously, the context has been established, now risks needing to be identified. This is a very important move of the risk assessment process, as any risks you fail to identify will not be handled A risk that has not been identified still exists and may create troubles later.

Four methods are usually used to identify risks [2]:

- Consultation with stakeholders - represent an outstanding method for identifying possible risks when orchestrating a risk assessment. The process generally involves deciding who the various stakeholders are who need to be questioned. Consultations may take place formally or informally and are usually excellent done personally; use of email can rush up the procedure.
- Physical inspection- of the site in which risks are being identified would be important, especially if a risk assessment has not been carried out before. A physical inspection requires seeing the sites in which the risk assessment is to be carried out and looking for all possible threats.

- Experience judgments – this process requires consulting specialists and expert information or perspective. Perspectives are based on a specific experience and knowledge in their field of expertise.
- Study of reports, information and data available. Many sources of information exist and can be used for the purposes of risk identification. These comprise information on equipment stating its size and restriction of use before it fails, or statistical reports on incidents occurring at public events and their nature. If proper documentation is kept of earlier projects, troubles or unfinished operations, this method can be used to review such documentation as:
  - lessons learned;
  - earlier risk management plans;
  - risk monitoring reviews;
  - problem or trouble lists.

c. **Analyze the risks**.

In order to analyze risks it is essential to have as much information about every risk as possible. This will enable more accurate assessment of likelihood and severity when deciding the level of risk exposure. Risk analysis presented in Table 1 involves combining the possible consequences or impact of an event with the likelihood of that event occurring. The result is a 'level of risk'. That is:

Level of risk = consequence x likelihood **(1)**

The more serious the risk, the more information should be collected and checked. In the first stages, determining whether the risk is high enough to demand more information may be a subjective judgment.

Table 1: Risk analysis - likelihood of event occurring

Consequence / **Likelihood**	*Extreme*	*Very high*	*Moderate*	*Low*	*Negligible*
Almost certain (A)	Severe	Severe	High	Major	Significant
Likely (B)	Severe	High	Major	Significant	Moderate
Moderate (C)	High	Major	Significant	Moderate	Low
Unlikely (D)	Major	Significant	Moderate	Low	Very low
Rare (E)	Significant	Moderate	Low	Very low	Very low

d. **Evaluate the risks**.

Once the level of risk has been settled for each risk, this information can be introduced onto a risk register or program showing the level of risks. The evaluation will decide the risk priority, displaying which risk must be operated first in order to minimize the exposure of the organization to serious loss; small or insignificant risks might be treated immediately where it would be quick and / or low cost to do so.

e. **Treat the risks**.

"Risk treatment is a decision making process. For each risk, risk treatment involves choosing amongst at least four options: accept the risk, avoid the risk, transfer the risk, or reduce the risk. In general, risks are treated by selecting and implementing measures designed to modify risk" [8]. Elaborate and implement a plan with specific counter-measures to address the identified risks, we have to consider [3]:

- Priorities (strategic and operational)
- Resources (human, financial and technical)
- Risk acceptance, (i.e., low risks)

Document your risk-management plan and describe the reasons behind selecting the risk and for the treatment chosen, record allocated responsibilities, monitoring or evaluation processes, and assumptions on residual risk. Low and very low level risks can normally be accepted, subject to on-going monitoring.

f. **Monitor and review**.

In admitting, prioritizing and managing risks, organizations make assumptions and conclusions established on circumstances that are liable to change.

Risk management policies and decisions must be usually reconsidered also managers have to check actions and procedures to determine the veracity of planning assumptions, and the ability of the measures adopted to treat the risk.

g. **Communication and consultation**.

Appropriate communication of risk and consultation with concerned parties are necessary to support risk-management decisions, actuality communication and consultation must take place at each stage of the risk-management process as well as on the process as a whole. Schematically, the risk-management process is depicted in the Figure 1:

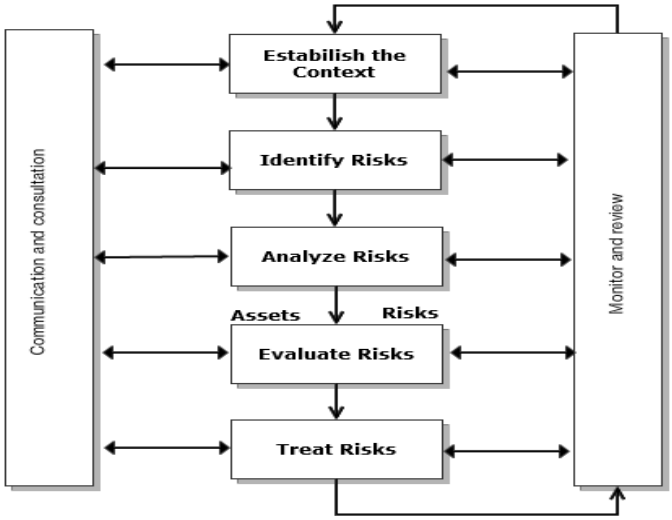

Figure 1 Risk management processes.

Why you should use risk management? The process helps Organizations center on priorities and in decisions on using limited resources to hand with the highest risks.

2. Public Key Infrastructure

Public key infrastructures (PKI) have become the starting point for modern security mechanisms on the Internet. PKI is closely linked to the asymmetric key encryption, digital signatures and encryption services, but to enable these services are used digital certificates. PKI facilitates storage and exchanges electronic data in a secure way; safety is ensured by using public key cryptography, and the types of security services offered [4]:

- Confidentiality - maintaining the private nature of the message is performed using the encryption and use the public key from a certificate to establish an encrypted communication channel is the result that only the recipient specified in the certificate (which is the owner of private key) will be able to decrypt the message encrypted.
- Integrity - proof that the message has not been altered is obtained with the help of digital signature, and by verifying the signature successfully, that message has not been altered after signing. Authenticity - verifying the identity of an individual or an application which transmits the message is done using a digital signature.
- Non-repudiation - property providing security as the certainty that the message cannot deny it later passed.

The services listed above are part of secure communications and these are an essential security requirement and dates from ancient times. In practical terms, this often means encrypting messages are transmitted in the Internet by email, file transfer; secure electronic transactions [5].
Public key infrastructure or PKI deal with key management encryption-decryption for different user groups to ensure confidentiality of information, more and check their integrity using digital signatures and non-repudiation, we could say that PKI is based on public key cryptography, digital signature and digital certificates.

3. PKI Risks

PKI is an excellent technology to help users certify that the people or companies. They are corresponding with are who they say they are. It has proven itself invaluable in e-commerce among other areas. As with any technology, however, it is not without its own security risks.

Although PKI is considered a must-have technology, like any other security solution is not 100% sure, and it has its own risks, but if we identify and mitigate, the result will be a strong security solution.

The possible risks and threats associated with PKI:

1. Legislation compliance;
2. Trust establishment;
3. Key generation;
4. Private key protection;
5. CRL availability.

1. Legislation compliance. At European level, the European Union created a set of guidelines, called EU Directives, which cover the area of Public Key Infrastructure. The directives associated with the concept of PKI are:

- EU Data Protection Directive
- EU Electronic Signatures Directive

Romanian legal frameworks for electronic signatures include [7]:

- Law on the Electronic Signature - no. 455/2001 and the technical and methodological norms of application approved by Government's Decision no 1259/13th of December, 2001.
- Government Decision no. 2303/14th of December 2004 on amendment of some acts of Information Technology.
- Minister Order no. 473 of June 9, 2009 on the procedure for granting, suspending and withdrawing accreditation decision of certification service providers.

2. Trust establishment. Establishing trust between groups of individuals remains a delicate problem. A trusted infrastructure, require an individual to trust unknown entities, or provide relatively low probabilistic guarantees of authenticity. Not everyone who possesses a digital certificate is actually trustable.[6]

3. Key generation. The generation of the public and private key is realized using a cryptographic algorithm, and the generation of a digital signature is realized using a hash algorithm. The risk related with the cryptographic or hash algorithm used to generate the keys or digital signature, concerns to the length of the keys that define the power of the algorithm. Almost always the risk of using weak algorithms exist, which can generate the public key from the private key in a way that lets the value of the private key to be decided. All authority must use well-known algorithms and a substantial bit length for the generated keys to stop an attacker from predicting the keys and causing troubles.

4. Private Key protection. A private key owner is responsible for getting all suitable insurances to secure their primary key and be sure that no one has access to it. This is important since anyone who obtains a user's private key can forge a message and claim it was sent by that user, and can decrypt any sensitive communications encrypted by that user's public key.

5. CRL availability. Numerous applications depend on certificate revocation list (CRL) availability and fail if the CRL is inaccessible or out-of-date because certificate revocation checking can prevent client access due to the inaccessibility or expiration of CRLs for each certificate in the certificate chain, and therefore, in the PKI implementation we have to consider for high availability of CRLs.

Conclusions

With the modifications in today's business environments and the switch from the traditional face-to-face business models, systems must be developed to guarantee that trusted relationships are preserved. PKI is widely accepted standard for encryption and authentication. Lots of applications such as SSL based web server, B2B applications, E-mails, S/MIME, can use PKI solutions. The implementation of a PKI is planned to provide tools to ensure trusted relationships are established and maintained. The specific security functions in which a PKI can provide are confidentiality, integrity, non-repudiation and authentication.

PKI is a preferred technology despite the risks that may arise from its management. Like any other technology, it depends on us to reduce and threats related to maximize the advantage offer. Recognizing in advance, we could prevent possible difficulties appear operate. Despite that we have to recognize the significance of PKI technology at an individual, business and national level, although Romania doesn't have one at the national level.

References

[1] AS/NZS ISO 31000, 2009. *Risk management - Principles and guidelines.* International Organization for Standardization.

[2] ISO/IEC Guide 73, 2002. *Risk management -Vocabulary-Guidelines for use in standards.* British Standards Institution.

[3] ISO/IEC 27001, 2005. *Security Management Standard.* British Standards Institution.

[4] V. Patriciu, M. Pietroşanu, I. Bica, J. Priescu, 2006. *Semnături electronice şi securitate informatică*. All.

[5] N. Vatră, 2009. *Public key infrastructure overview*. Scientific Studies and Research, Series Mathematics and Informatics, no. 2, vol. 19, pp.471 - 478.

[6] R. Vacca, 2004. *Public Key Infrastructure: Building Trusted Applications and Web Services*, 1 edition Auerbach Publications.

[7] Internet law, 2010. *Legislation on electronic signatures*.[Online] Available at: http://www.legi-internet.ro/legislatie-itc.html [Accessed 17 May 2010].

[8] PRAXIOM RESEARCH GROUP LIMITED. *Definition Risk treatment, Internet*, 2010. [Online] Available at: http://www.praxiom.com/iso-27001-definitions.htm [Accessed 17 May 2010].