SECURITY RISK IN DISTRIBUTED ENVIRONMENTS

Valentin MEȚGHER[1], Vasile GÎSCĂ[2]
Technical University of Moldova
168, Stefan cel Mare bvd.
Chişinău, MD-2004,Republic of Moldova
[1]vmetgher@hotmail.com ,[2] gasca@mail.utm.md

Abstract. *Conventional risk analysis techniques focus on a single environment and are inappropriate to be used in distributed ones. This article is an analysis of the changing environment for today's organizations and the requirements to have a risk management approach in distributed environments where the single common point for the organizations involved in a joint effort is the mission which needs to be achieved.*

Keywords: *risk, security, mission, survivability, distributed environment.*

Introduction

Organizations are increasingly being confronted with security incidents in great numbers. These incidents are not only more prevalent, but they represent a wide range of motives and intended consequences.

It becomes more evident that improvement in security requires to change old perceptions and to define new targets. Security is not an isolated discipline and it lives in the organisational context.

So, security must take into account the *dynamically changing risk environment* in which organisations are expected to survive and operate.

With the global increase of threats in business environment, there is high demand for the systems supporting the operation of the organizations to exhibit *survivability attributes* in achieving their mission.

Survivability is defined as the capability of a system to fulfil its mission, in a timely manner, in the presence of attacks, failures, or accidents [1].

It is important to recognize that it is the mission fulfilment not any particular subsystem or system component that must survive. Central to the notion of survivability is the capability of a system to fulfil its mission, even if significant portions of the system are damaged or destroyed.

To achieve and sustain an adequate level of security that directly supports the mission of the organization, senior management must shift their point of view and that of their organization from an *information-technology-based*, *security-centric*, *technology-solution perspective* to an *enterprise-based*, *risk management*, *organizational continuity* and *resilience perspective*.

There are six shifts in thinking on security as being enterprise driven [2]

Table 1: Shifting Security Perspectives

Area	Shifting From	Shifting To
Security scope	Technical	Organizational
Ownership of security	Information technology	Organization
Focus of security	Discontinuous and intermittent	Integrated
Funding for security	Expense	Investment
Security drivers	External	Internal
Security approach	Ad hoc	Managed

To make things more complex, in modern business environment, a workflow is no longer exclusively contained within organizational boundaries. In fact, management control of work processes is often distributed among multiple organizations or groups.

Today it is common for multiple organizations to pool appropriate resources in pursuit of a single mission and bring together a diverse set of skills without regard to physical location. This is especially true during the last decade with increasing outsourcing of internal business processes.

The organizations have in common the *mission* which they have to achieve rather than the same organization chart.

They must now be prepared to identify and address risks inherited from activities done by other organizations and attempt to minimize the risks they impose on downstream activities.

It requires a collaborative management approach that includes the *ability to coordinate the risk management activities of multiple organizations in achieving the mission*.

Defining Risk

Risk can be defined, in the context of the organization's mission threats, as the *possibility of suffering harm or loss*.

The term Risk management incorporates all the activities required to identify and control the exposure to risk that may have an impact on the achievement of the organization's mission.

It also provides the means for anticipating and addressing the numerous obstacles that can get in your way. When you follow a risk management approach, you put yourself in position to achieve your objectives through informed and proactive decision making.

Risk Management is an important aspect in organization's development and operation, whether related to putting the right effort in place in achieving its mission or implementing of Information Security Management System to protect its information assets.

There are two distinct phases: risk analysis and risk management.

Risk analysis is concerned with gathering information about exposure to risk so that organization can make appropriate decisions and manage risk appropriately.

Management of risk involves having processes in place to monitor risks, access to reliable and up-to-date information about risks, the right balance of control in place to deal with those risks, and decision making process supported by a framework of risk analysis and evaluation [3].
Risk analysis allows to determine an acceptable level of risk and selection of the necessary protection actions for risk reduction.
While allocating the effort for mitigating the risk, it is important to assess the potential of risk reduction versus the associated costs, having a final goal of keeping the risk at an acceptable level of tolerance. The tolerance of the operational risk is the maximum acceptable exposure in regard to the operational risk, taking into account the costs and benefits involved (Fig.1)

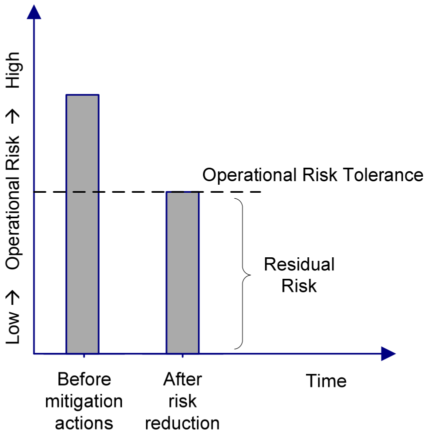

Figure 1 Residual risk.

For each identified risk according to risk assessment, it is necessary to adopt decisions of **risk treatment** which can include: i) applying the necessary controls for risk mitigation; ii) accepting the risk according to existing criteria; iii) transferring the risk to other entities.
No control can offer absolute security; instead management should determine and accept responsibility for residual risk tolerance.

Table 2 reflects the risk analysis and risk treatment outcomes, finally obtaining the residual risk.

Table 1. Example of risk treatment

Asset	Threat	Probability	Impact (cost)	Risk Factor	Actions	Residual Risk Factor
Notebook	being stolen	0.5	5	2.5	Working procedure with mobile equipment	0.5
PC	fire	0.2	1	0.2	Staff training	0.1

Risk in distributed environments

Inside an organization, when the manager has oversight of the entire lifecycle of a project and can control all the processes, he/she has considerable flexibility and control to make decisions, reallocate people from one process to another and mitigate the risks in order to achieve the mission.

However, the situation changes in a more complex environment where the processes are distributed among multiple organizations that have the same mission.

In distributed processes, management from each organization controls its piece of the overall process, and, in most cases, no one has management authority over the end-to-end workflow.

And most contracts do not mandate a common approach for managing risk; instead they give each manager considerable autonomy in this regard. As a result, there tends to be a lack of uniform operational risk tolerance in most distributed processes, as illustrated in Fig. 2.

The operational risk affecting a given activity in a distributed process influences the risk affecting all subsequent activities. As a result, all managers need to be aware of the risk they inherit from upstream activities and, in turn, impose on downstream activities.

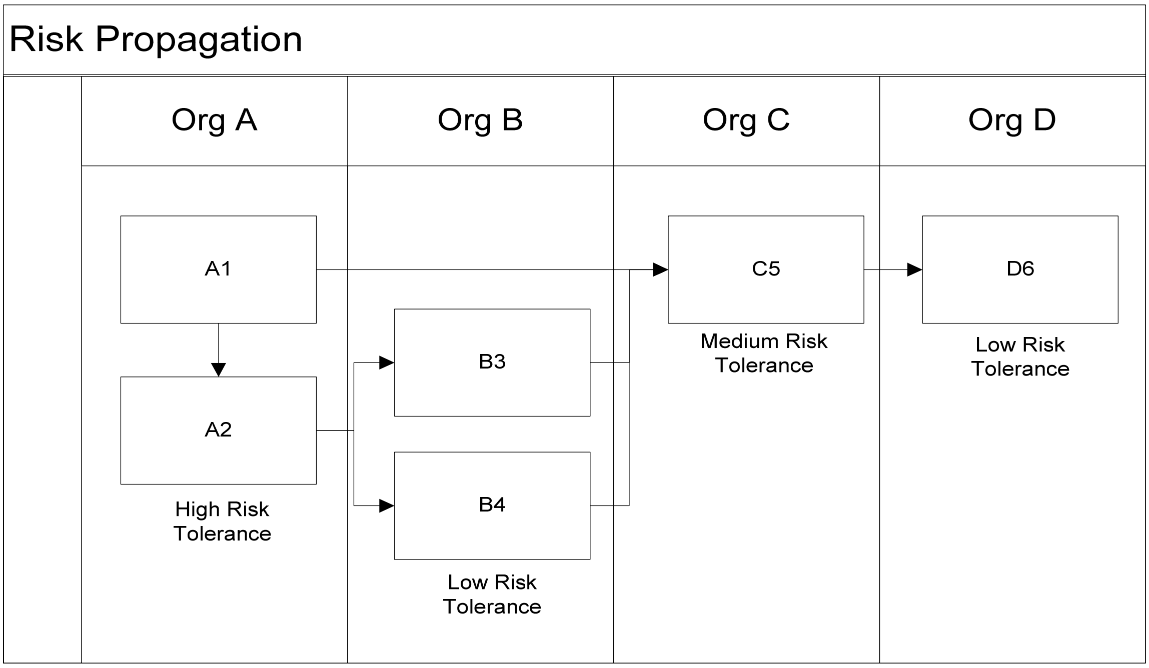

Figure 2. Risk Propagation.

The realities of the modern business environment are:

- o Many entities can work together to achieve a single mission;
- o Any entity can support multiple missions;
- o Many entities can support a single mission, and each entity can support multiple missions at any given time.

In a distributed environment it makes sense to frame the risk around the mission to serve as a good base for risk analysis.

Mission helps to define the *scope of the risk analysis activities*. One of the key products of risk analysis activities is an *operational risk profile of the mission*, which essentially provides a snapshot of how operational risk can affect a given mission. It is developed by analyzing process performance in a variety of operational situations.

A complete profile must include the following three key components: a *risk causal chain*, a *measure of the mission's operational risk exposure*, and the *key risk drivers* as defined in the MAAP protocol [4].

Risk drivers are the sources of risk having the strongest influence on the overall risk to the mission. They form multiple critical paths throughout the causal chain and provide a natural starting point when developing risk mitigation strategies.

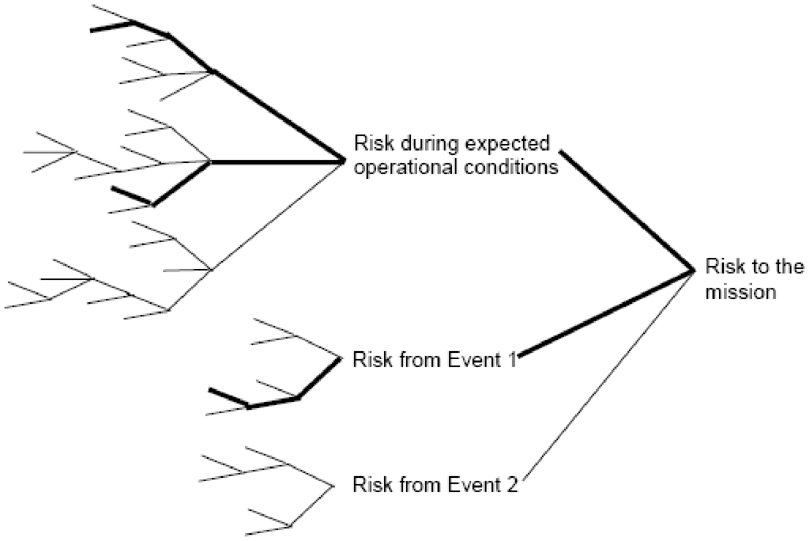

Figure 3. Key risk drivers.

The following guidelines define the framework for risk management in distributed processes [4]:

- o Determine mission objectives.
- o Characterize all operations conducted in pursuit of the mission (processes, roles, etc.).
- o Define common, for different organizations, risk evaluation criteria in relation to the mission objectives.
- o Identify potential failure modes (when process performance deviates from the expected one).
- o Perform a root cause analysis for each failure mode.
- o Develop an operational risk profile of the mission (critical path analysis of the risk causal chain).
- o Ensure that operational risk is within tolerance.

The operational risk profile is designed to provide information on a number of organizational levels both at the strategic and the operational levels.

The benefits are, that managers are presented with a measure of their mission's operational risk exposure, which provides insight into the effectiveness of the underlying work process. At the same time, staff members are provided with a detailed risk causal chain, including which causes are driving the overall risk to the mission.

This detailed information is used in forming mitigation strategies to reduce operational risk to an acceptable level and improve mission assurance in an environment where multiple processes spread over many organizations work towards a common goal - achieving the mission.

Conclusions

Conventional risk analysis techniques focus on a single environment and are inappropriate to be used in multiple ones.

New techniques are required for risk management in a distributed environment. Key is the fact that risk analysis is done and driven by the mission common to all organizations.

This is the unifying element that serves as a platform for the risk assessment in distributed environments.

References

[1] Ellison, Robert; Fisher, David (1997). *Survivable Network Systems: An Emerging Discipline*. SEI. Carnegie Mellon University.

[2] Richard A. Caralli (2004). *Managing for Enterprise Security*. Networked Systems Survivability Program. Carnegie Mellon University.

[3] Office of Government Commerce (2004). *Management of Risk. Guidance for Practitioners*. TSO

[4] Christopher J. Alberts, Audree J. Dorotee (2005). *Mission Assurance Analysis Protocol (MAAP).* Software Engineering Institute. Carnegie Mellon University.