SHIFTING SECURITY MANAGEMENT PERSPECTIVES

MEŢGHER Valentin

Technical University of Moldova, CIM

Abstract: Security has become one of the most urgent issues for many organizations. It is an essential requirement for doing business in a globally networked economy and for achieving organizational goals and mission. Organizations can no longer be effective in managing security from the technical perspectives. This article is an analysis over the existing security challenges at the enterprise level; presents a view of the changing environment in which security must be performed and new approaches of achieving this.

Key words: Security, risk management, mission, change, survivability.

1. INTRODUCTION

Organizations are 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. The importance of these attacks is not that they target the organization's technical infrastructure or physical premises; instead, it is the interruption of the affected organization's plan to accomplish its mission that matters.

A technology-driven perspective on security obscures the fact that the productive elements of the organization – people, assets, and processes – are the real focus of a protection strategy. Enterprise-wide issues that affect the organization's ability to accomplish its mission require organization-driven solutions.

Organizations are not setting meaningful security goals and are not able to know when and if they've reached the goals they do set. The current trends indicate that the organisations continue to address security tactically rather than strategically, focusing primarily on aspects such as vulnerability analysis, perimeter security and failure of senior management to recognize the value of security and its contribution to reduce risks from the main processes and risks related to the primary mission of the organisation.

Security in modern environment requires a shift from the traditional technical centric approach to the one which is considered at the enterprise level and is closely linked with business strategy and the mission of the organisation.

2. SHIFTING SECURITY PERSPECTIVES

It becomes more evident that improvement in security requires changing old perceptions and defining 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.

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 [1]

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

Security resilience

A key question the organisations will ask is why they need security. The effort of organisations could be characterised as reactive, assigning resources to fix the gap according to the latest announcement of vulnerabilities, but without identifying the real impact and establishing the balance between the need and cost.

Security shall contribute to the organisation of being able to adapt to the changing risk and environment and still be able to perform its mission. The main goal thus is to sustain organisation's *resiliency*, defined as - the ability to stretch beyond the limits and return back to its initial state. [1] Resiliency can be regarded as survivability of the organisation.

Survivability is defined as the capability of a system (or organisation in this case) to fulfil its mission, in a timely manner, in the presence of attacks, failures, or accidents. [2]

Security needs to be positioned as an enabler of the organization—it must take its place alongside key productive areas such as: HR, finances, main sound business processes as the elements of success for accomplishing the mission.

Risk Management

Risk Management is the process of identifying, controlling, and mitigating risks. It includes: risk assessment, cost benefit analysis, and the selection, implementation, testing and evaluation of security.

Risk and security are important parts of organizational resiliency. Risk management is a primary function of all organizations. A risk management approach to security is a step toward aligning security with strategic drivers.

Maturity level of security practices

There exist different levels of applying the security practices in organisations from a low to high focus. Depending on the company needs in protecting the key assets and supporting its objectives, to an extent, one or both of them could be adequately applicable.

The levels of the maturity of security practices from low to high could be regarded as:

- *Ad hoc* – Lack of defined security strategy, policies.
- *Vulnerability based* – Vulnerability focus and reacting on them.
- *Risk based* – Focus on critical assets, their threats and mitigation actions.
- *Enterprise based* – aligns security and organisation's strategy to achieve organisation resiliency.

3. BEST PRACTICES

Among best practices ensuring applicability of the security at the enterprise level are *BS-7799, ITIL*, and other government, defence or community driven practices.

BS-7799

The standard focuses on establishing of an Information Security Management System (ISMS) in the organisation, which is - a systematic approach to managing sensitive company information so that it remains secure. By registering the ISMS the organisation can demonstrate to its stakeholders that ISMS meets the requirements of the standard.

The ISMS contains 10 areas of security [3]: *Security policy; Organisation of assets and resources Asset classification and control; Personnel security; Physical and environmental security; Communications and operations management; Access control; Systems development and maintenance; Business continuity management; Compliance*

The BS7799 represent a complex view over the methods of implementing and assuring security of information at the enterprise level.

ITIL

IT Infrastructure Library is a set of best practices applied in IT service management. It provides a framework for effective operations of the IT services in a company and presents the application of security for the infrastructure; also applying the security when building new applications.

4. CONCLUSIONS

In the increasingly threats sophistication environments, organisations can no longer have an effective security management based only on technical approach. Security is a business problem regarded at the enterprise level. It requires the organisation with the support from senior management to shift from a single discipline approach towards a security management one. This fact will ensure adequate security is in place first of all to meet the business objectives, support its mission and that organisation is resilient in the changing environment.

5. REFERENCES

[1] Richard A. Caralli (2004). *Managing for Enterprise Security.* Networked Systems Survivability Program. Carnegie Mellon University.
[2] Ellison, Robert; Fisher, David (1997). *Survivable Network Systems: An Emerging Discipline*. SEI. Carnegie Mellon University.
[3] *Information security management systems - Specification with guidance for use*. British Standards Institution.