Risk Assessment

Authors: Tommaso Puccetti, Edoardo Dini

Università degli studi di Firenze

22/09/2018

IT Security Management: overview (1)

Is the formal process of answering the questions:

- Ensure that asset are sufficiently protected in a cost-effective manner;
- Security risk assessment is needed for each asset in the organization; that require protection;
- Provide the information necessary to decide what management, operational and technical controls are needed to reduce the risk identified

IT Security Management: overview (2)

Definition:

A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security management functions include:

- determining organizational IT security objectives, strategies, and policies
- determining organizational IT security requirements
- identifying and analyzing security threats to IT assets
- identifying and analyzing risks
- specifying appropriate safeguards
- monitoring the implementation and operation of safeguards
- developing and implementing a security awareness program
- detecting and reacting to incidents

IT Security Management: a cyclic process

It is important to emphasize that:

- IT security management needs to be a key part of an organizations overall management plan.
- IT security risk assessment process should be incorporated into the wider risk assessment of all the organizations assets and business processes.
- IT security management is a cyclic process **that must be repeated constantly** (as specified in [ISO27001]).

Figure 14.2

Figure 14.1

Evolution and consensus

The discipline of IT security management has evolved considerably over the last few decades. This has occurred in response to the rapid growth of, and dependence on networked computer systems and the associated rise in risks to these systems. In the last decade a number of national and international standards have been published. These represent a consensus on the best practice in the field. The International Standards Organization (ISO) has revised and consolidated a number of these standards into the 27000 series.

ISO 27000 series of Standards on IT Security Techniques

27000:2012	Information security management systemsOverview and vocabulary provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2005	Information security management systemsRequirements specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System.
27002:2005	Code of practice for information security management provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	Information security management system implementation guidance details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	Information security managementMeasurement provides guidance to help organizations measure and report on the effectiveness of their Information Security Management System processes and controls.
27005:2011	Information security risk management provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2007	Requirements for bodies providing audit and certification of information security management systems specifies requirements and provides guidance for these bodies.

Organizational Context and Security Policy

In IT security management process comprises an examination of the organization's IT security **object, strategies and policies**. This can only occur in the wider context of the organization's management. IMMAGINE SLIDE 8

Security Objectives

- What key aspects of the organization require IT support in order to function efficiently?
- What tasks can only be performed with IT support?
- Which essential decisions depend on the accuracy, currency, integrity, or availability of data managed by the IT systems?
- What data created, managed, processed, and stored by the IT systems need protection?
- What are the consequences to the organization of a security failure in their IT systems?

Security Strategy

Once the objectives are listed, some broad strategy statements can be developed. These outline in general terms how the identified objectives will be met in a consistent manner across the organization:

- The topics and details in the strategy statements depend on the identified objectives, the size of the organization, and the importance of the IT systems to the organization.
- The strategy statements should address the approaches the organization will use to manage the security of its IT systems. Given the organizational security objectives and strategies, an organizational

Security Policy

Given the organizational security objectives and strategies, an organizational security policy is developed that describes what the objectives and strategies are and the process used to achieve them.
INSERIRE ELENCO PUNTATO

Management Support

IT security policy must be supported by senior management Need IT security officer

- To provide consistent overall supervision
- Liaison with senior management
- Maintenance of IT security objectives, strategies, policies
- Handle incidents
- Management of IT security awareness and training programs
- Interaction with IT project security officers

Large organizations need separate IT project security officers associated with major projects and systems

Security Risk Assessment

IMMAGINE SLIDE 11

Baseline Approach

FARE IMMAGINE COME PER I SUCCESSIVI 2 APPROCCI IN MODO CHE SIANO CONSISTENTI

- Goal is to implement agreed controls to provide protection against the most common threats
- Forms a good base for further security measures
- Use industry best practice
  - Easy, cheap, can be replicated
  - Gives no special consideration to variations in risk exposure
  - May give too much or too little security
- Generally recommended only for small organizations without the resources to implement more structured approaches

Informal Approach

FARE IMMAGINI

Detailed Risk Analysis

FARE IMMAGINI

Combined Approach (1)

IMMAGINE Aim is to provide reasonable levels of protection as quickly as possible then to examine and adjust the protection controls deployed on key systems over time: Over time, this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems

Combined Approach (2)

1. Approach starts with the implementation of suitable baseline security recommendations on all systems
2. Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment
3. A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements
4. Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted

Detailed Security Risk Analysis (1)

INSERIRE IMMAGINE SLIDE 16

Detailed Security Risk Analysis (2)

INSERIRE IMMAGINE SLIDE 17

Establishing the Context (1)

- Initial steps
  - Determine the basic parameters of the risk assessment
  - Identify the assets to be examined
- Explores political and social environment in which the organization operates
  - Legal and regulatory constraints
  - Provide baseline for organizations risk exposure
- The **risk appetite** is the level of risk the organization views as acceptable

Establishing the Context (2)

INSERIRE IMMAGINE SLIDE 19

Terminology

- **Asset**: a system resource or capability of value to its owner that requires protection.
- **Threat**: a potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the assets owner
- **Vulnerability**: a flaw or weakness in an assets design, implementation, or operation and management that could be exploited by some threat
- **Risk**: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the assets owner.

Asset Identification

"What assets we need to protect?"

- These assets need to be identified and their value to the organization assessed.
- The ideal is to consider every conceivable asset, in practice this is not possible. Rather the goal here is to identify all assets that contribute significantly to attaining the organizations objectives and whose compromise the organizations operation.
- A security experts may not have an high knowledge of the organization's oepration and structure, so experts for each area of the organization are needed for the process.

Threat Identification (1)

"Who or what could cause harm to the assets?"

- Identifying possible threats and threat sources requires the use of a **variety of sources**, along with the experience of the risk assessor.
- Organizations define threat scenarios to describe how the tactics, techniques, and procedures employed by an attacker can contribute to, or cause, harm.

Threat Identification (2)

1. **Motivation**: Why would they target this organization; how motivated are they?
2. **Capability**: What is their level of skill in exploiting the threat?
3. **Resources**: How much time, money, and other resources could they deploy?
4. **Probability of attack**: How likely and how often would your assets be targeted?
5. **Deterrence**: What are the consequences to the attacker of being identified?

Vulnerability Identification

- Identify exploitable flaws or weaknesses in organizations IT systems or processes
  - Determines applicability and significance of threat to organization
- Need combination of threat and vulnerability to create a risk to an asset
- utcome should be a list of threats and vulnerabilities with brief descriptions of how and why they might occur

Analyze Risks

- Specify likelihood of occurrence of each identified threat to asset given existing controls
- Specify consequence should threat occur
- Hard to determine accurate probabilities and realistic cost consequences
- Use qualitative, not quantitative, ratings
- Derive overall risk rating for each threat

Definition:

Risk = probability threat occurs x cost to organization