Chapter 14: IT Security Management and Risk Assessment

Authors: Tommaso Puccetti, Edoardo Dini

Università degli Studi di Firenze

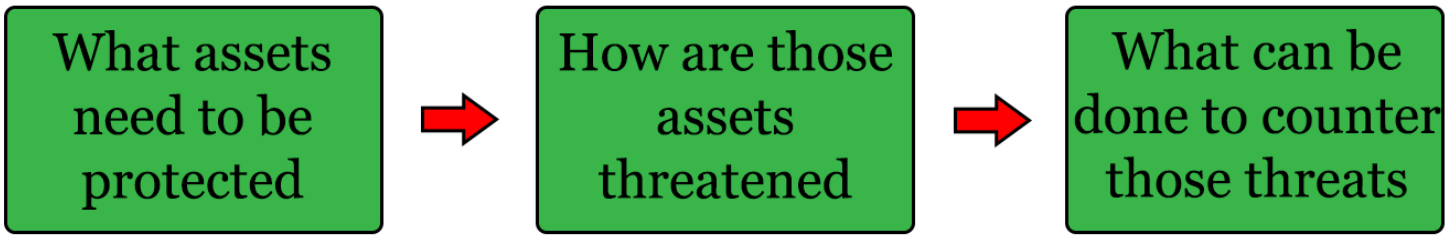
11/12/2018

Index

Index

IT Security Management: overview (1)

Is the formal process of answering the questions:



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

IT Security Management: overview (2)

Definition:

IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability.

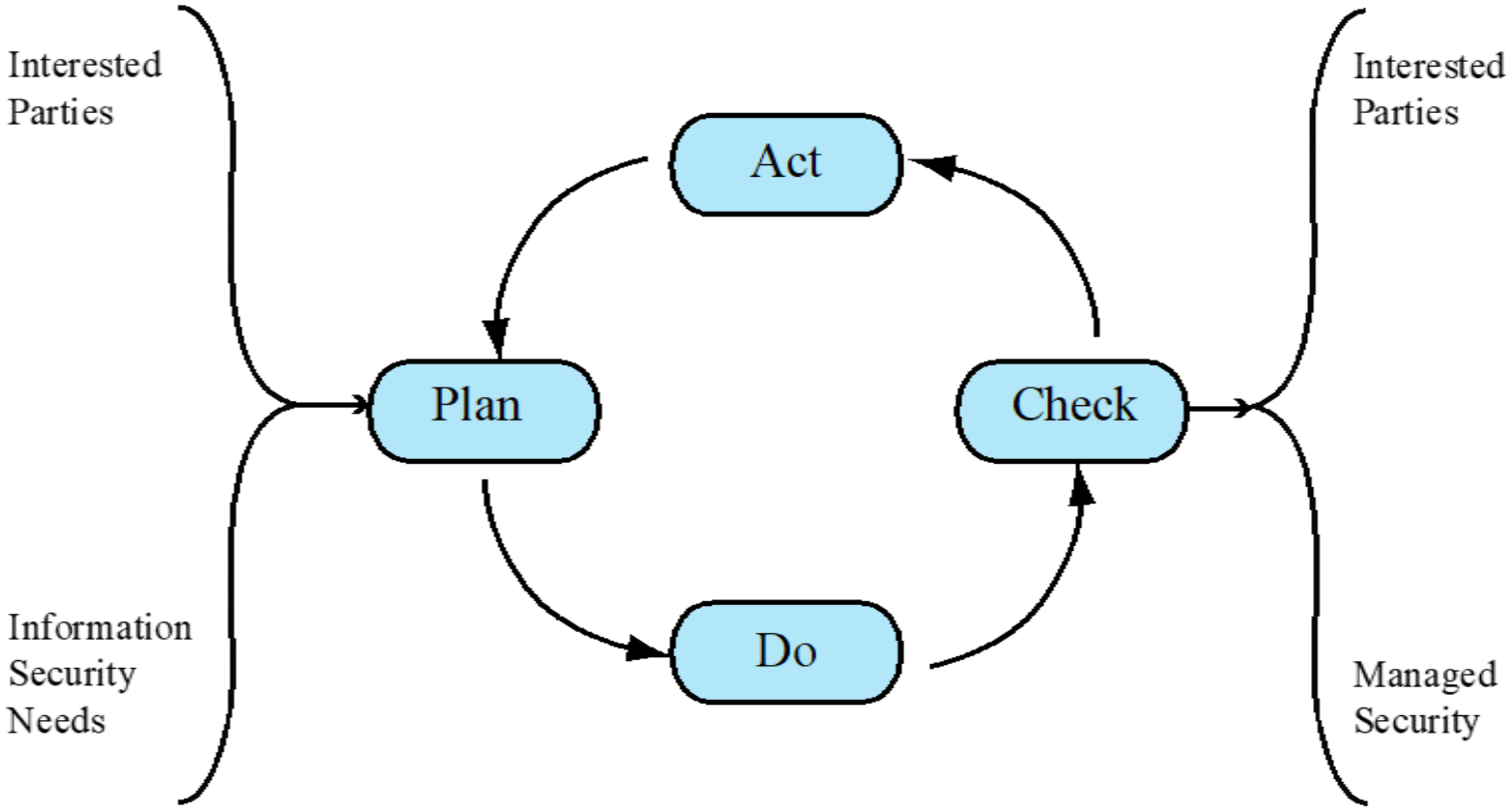
- Determining organizational IT security objectives, strategies, and policies;
- Determining organizational IT security requirements;
- Identifying and analyzing security threats to IT assets;
- Identifying and analyzing risks;
- Specifying appropriate safeguards;
- Monitoring the implementation and operation of safeguards;
- Developing and implementing a security awareness program;
- Detecting and reacting to incidents.

IT Security Management: a cyclic process (1)

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]).

IT Security Management: a cyclic process (2)



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 systems: Overview 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 systems: Requirements" 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 management: Measurement" 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.

Index

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.

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.

Security Policy (1)

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.

- The scope and purpose of the policy;
- The relationship of the security objectives to the organizations legal and regulatory obligations, and its business objectives;
- IT security requirements in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability, particularly with regard to the views of the asset owners;
- The assignment of responsibilities relating to the management of IT security and the organizational infrastructure;
- The risk management approach adopted by the organization;

Security Policy (2)

- How security awareness and training is to be handled;
- General personnel issues, especially for those in positions of trust;
- Any legal sanctions that may be imposed on staff, and the conditions under which such penalties apply;
- Integration of security into systems development and procurement;
- Definition of the information classification scheme used across the organization;
- Contingency and business continuity planning;
- Incident detection and handling processes;
- How and when this policy should be reviewed;
- The method for controlling changes to this policy.

Management Support

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

- To provide consistent overall supervision;
- Connection 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.

Index

Security Risk Assessment

Baseline Approach

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

Involves conducting an informal, pragmatic risk analysis on organization's IT systems

Exploits knowledge and expertise of analyst

Fairly quick and cheap

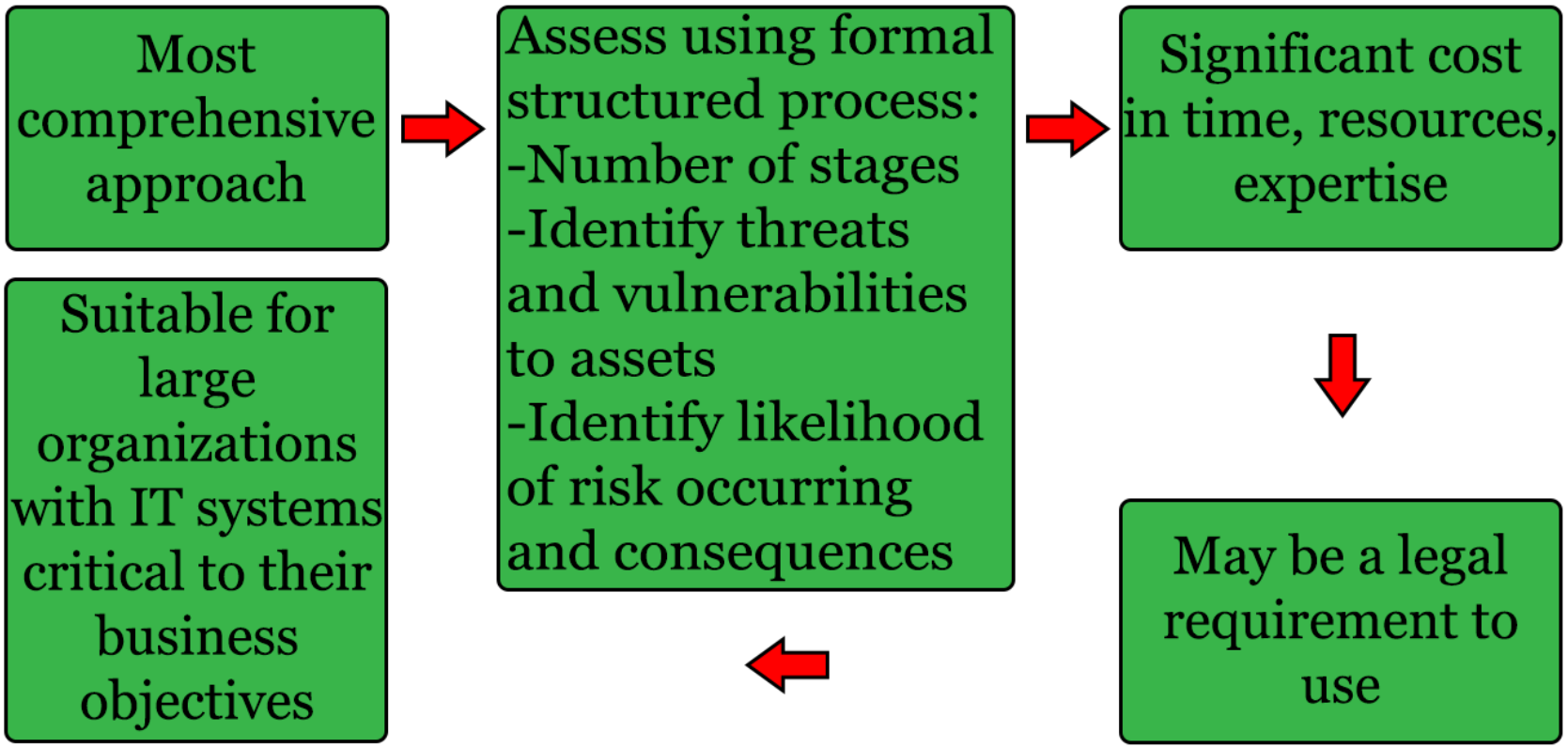
Judgments can be made about vulnerabilities and risks that baseline approach would not address

Some risks may be incorrectly assessed

Skewed by analyst's views, varies over time

Suitable for small to medium sized organizations where IT systems are not necessarily essential

Detailed Risk Analysis

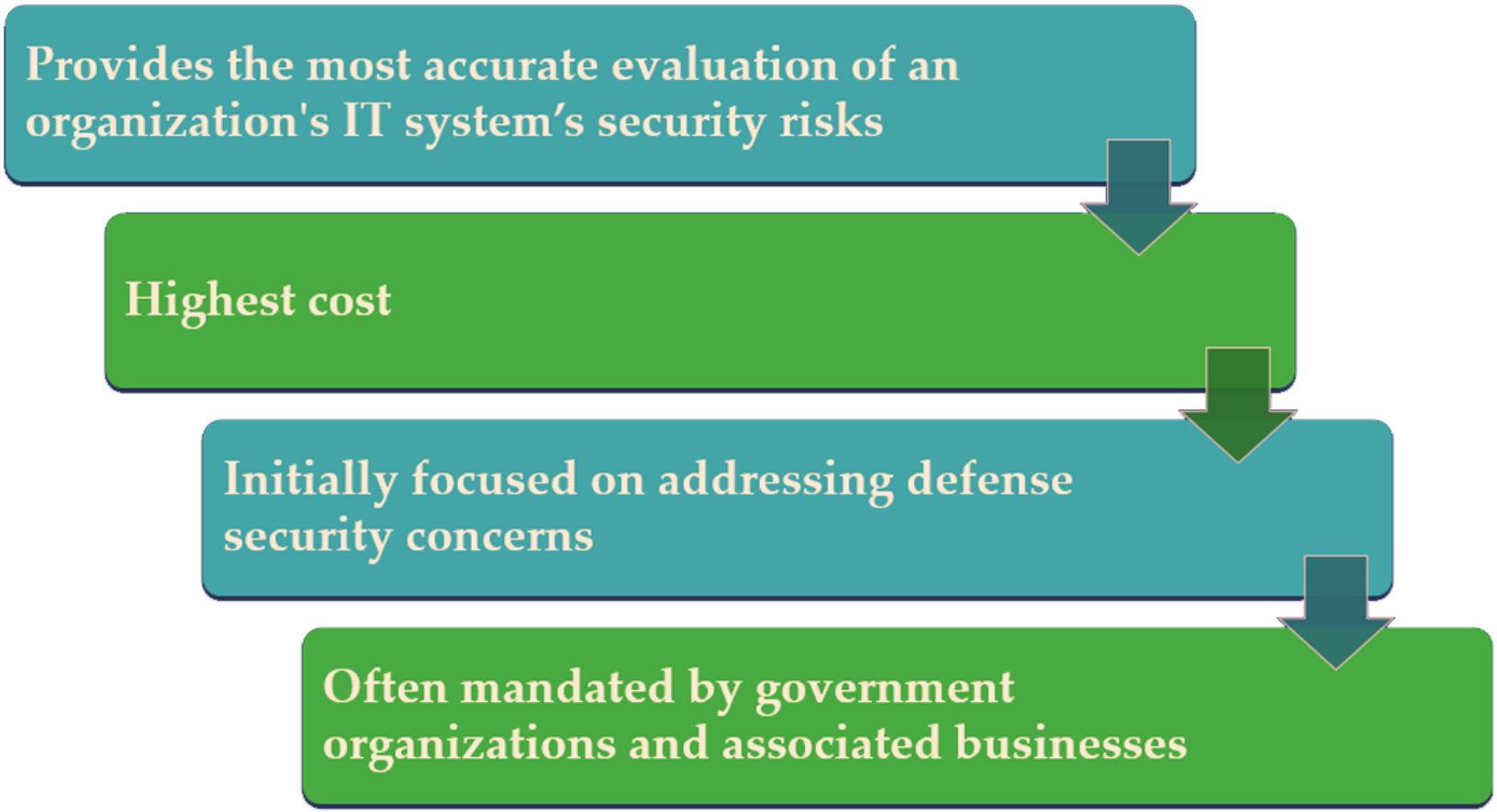


Combined Approach

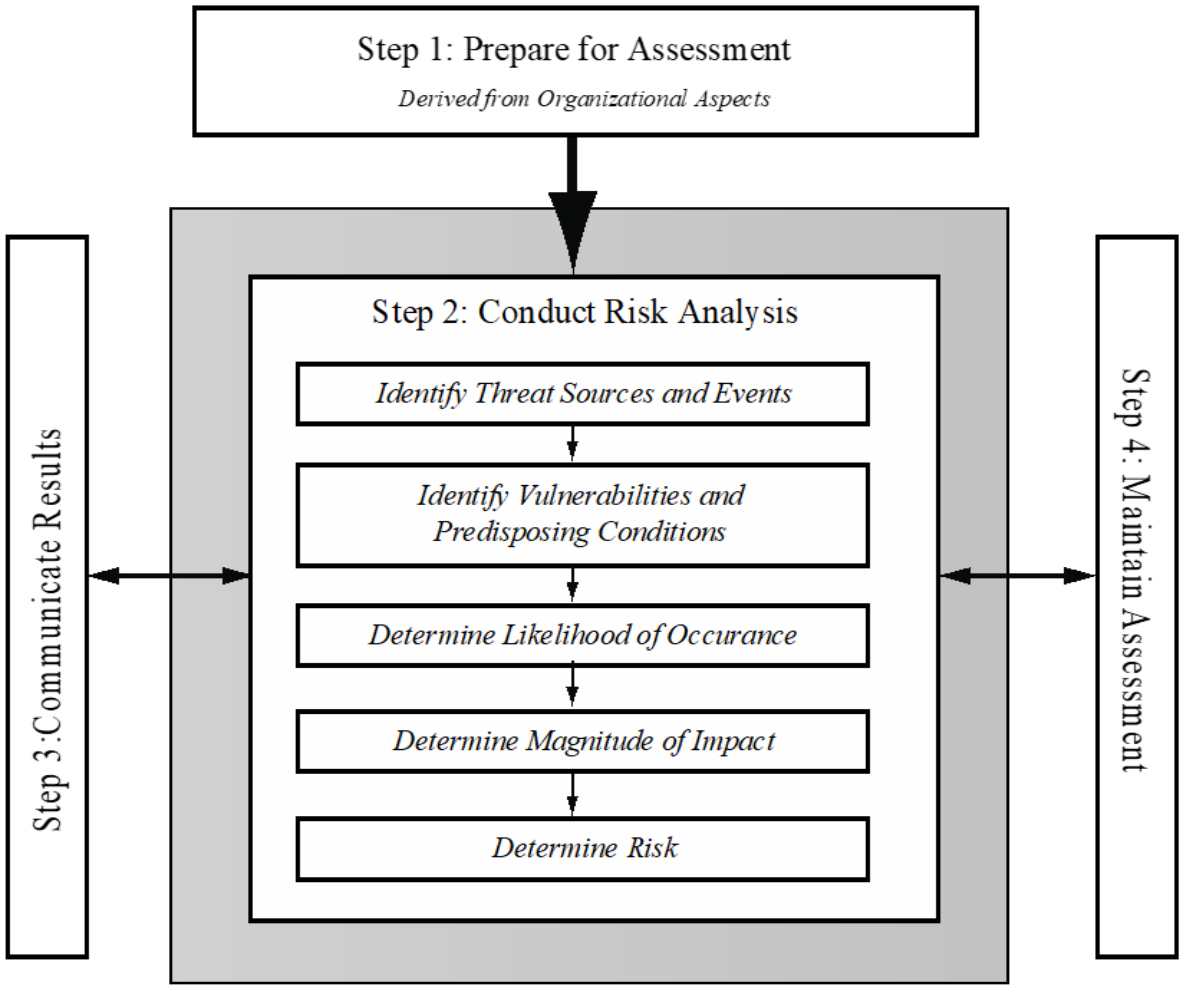
1. This approach starts with the implementation of suitable baseline security recommendations on all systems;
2. Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high-level risk assessment;
3. A decision can then be made to possibly 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.

Index

Detailed Security Risk Analysis (1)



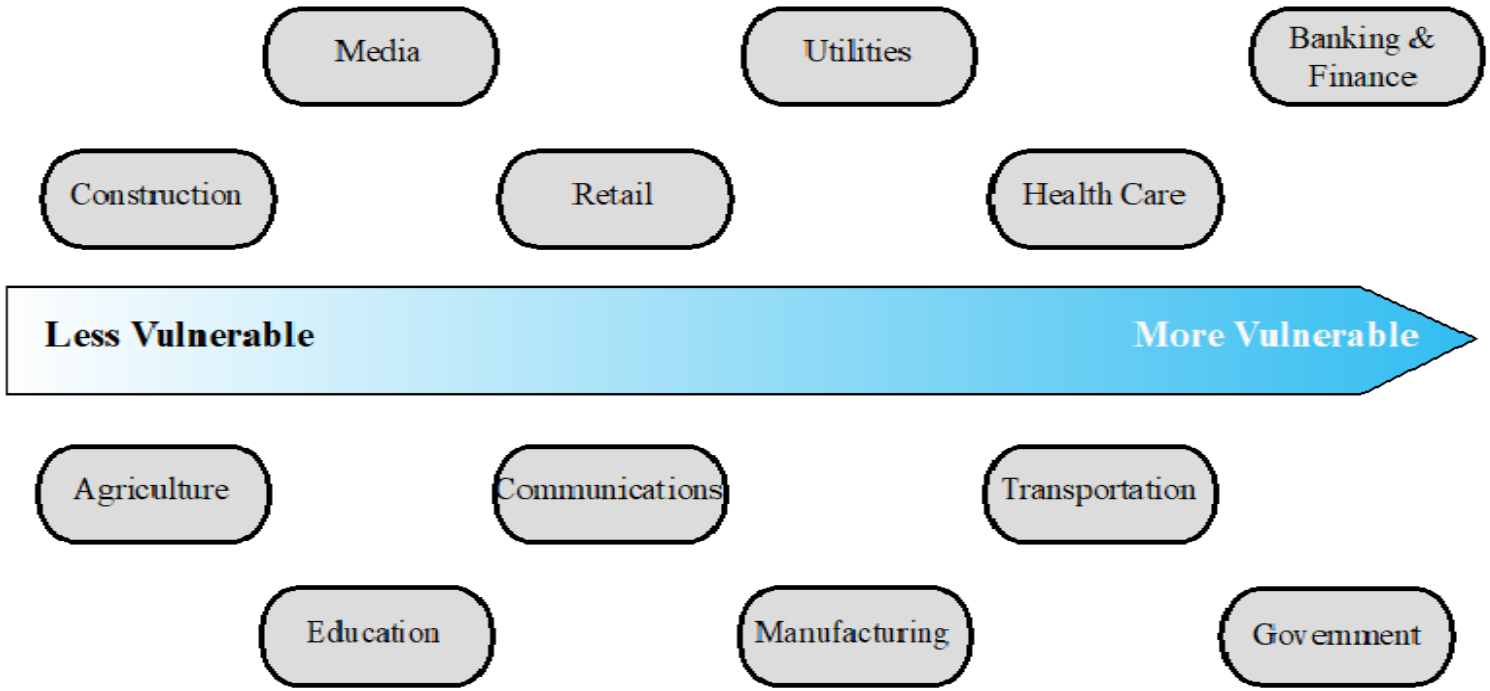
Detailed Security Risk Analysis (2)



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)



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 expert may not have an high knowledge of the organization's operation and structure, so experts for each area of the organization are needed for the process.

Threat Identification (1)

Threat Identification (2)

"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 (3)

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

"How could this occur?"

- **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;
- **Outcome** 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

Risk Likelihood (1)

- Take the assets and the threath/vulnerability from the previous steps and decides an appropriate rating. It is related to the **likelihood of a specified threath exploiting one or more vulnerability to an asset**;
- When deliberate **human-made threat** sources are considered, this estimate should include an evaluation of the attackers intent, capability, and specific targeting of this organization (an high rating suggests that a threat has occurred sometimes previously);

Risk Likelihood (2)

- There will very likely be some uncertainty and debate over exactly which rating is most appropriate. The final decision will be taken by the management;
- The likelihood is typically described **qualitatively**, using values and descriptions such as those shown in the table.

Rating	Likelihood Description	Expanded Definition
1	Rare	May occur only in exceptional circumstances and may be deemed a unlucky or very unlikely.
2	Unlikely	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	Possible	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	Likely	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	Almost Certain	Is expected to occur in most circumstances and certainly sooner.

Risk Consequences (1)

- Consequence specification indicates the impact on the organization (and not only on the security system) should the particular threat in question actually eventuate;
- Use **qualitative values**;
- As with the likelihood ratings, there is likely to be some **uncertainty** as to the best rating to use;
- As with the likelihood ratings, the consequence ratings must be determined **knowing the organizations current practices** (existing backup, disaster recovery, and contingency planning), will influence the choice of rating.

Risk Consequences (2)

Rating	Consequence	Expanded Definition
1	Insignificant	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	Minor	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	Moderate	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.

Risk Consequences (3)

Rating	Consequence	Expanded Definition
4	Major	Ongoing systemic security breach. Impact will likely last 48 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	Catastrophic	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	Doomsday	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

Risk level determination and meaning

	Consequences					
Likelihood	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk is expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls is likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Risk Register

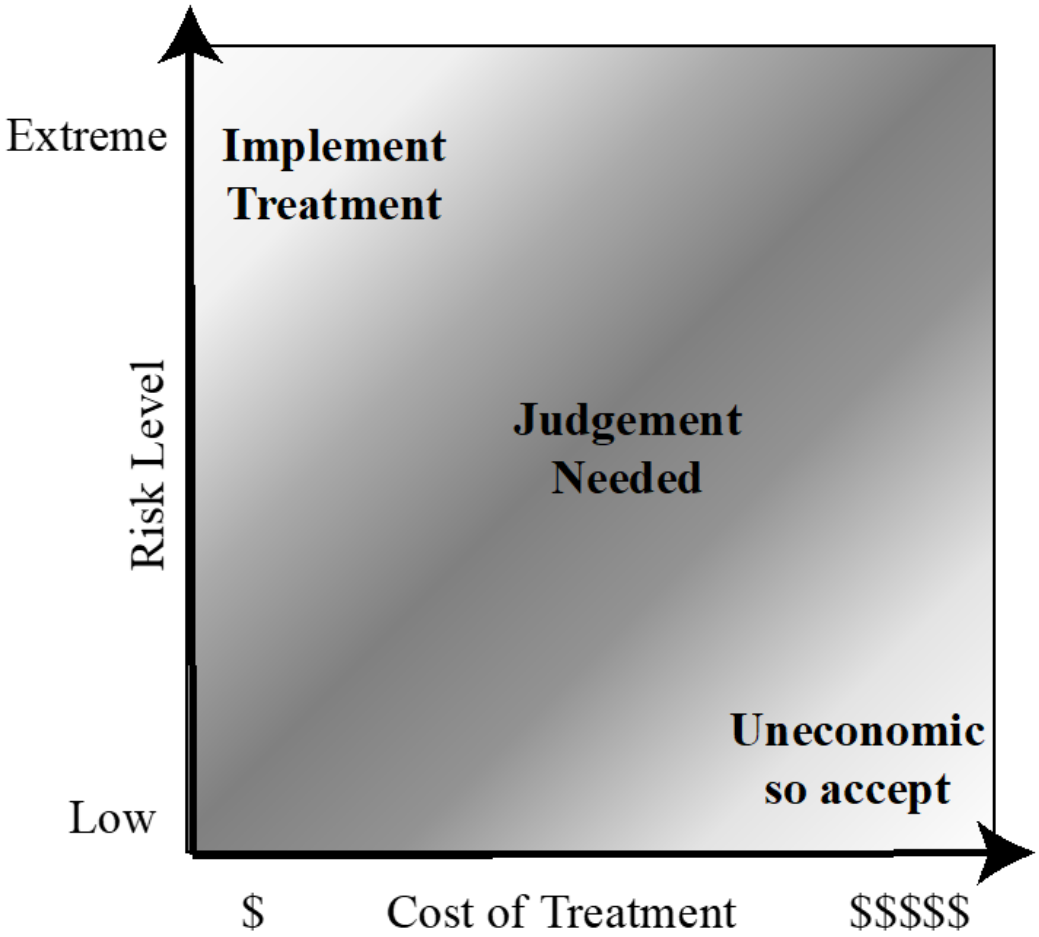
- Used to **keep track of the risk analysis process** and, if needed, provides evidence that a formal risk assessment process has been followed;
- The risks are usually sorted in decreasing order of level. This would be supported by details of how the various items were determined, including the rationale, justification, and and supporting evidence used.

Asset	Threat / Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside Hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment (1)

- Management decides which treatments should be apllied, considering the data collected in the previous phases;
- The decision is conditioned by two factors:
  1. Level of risk;
  2. Cost for treatment implementation.
- If the cost of treatment is high, but the risk is low, then it is usually uneconomic to proceed with such treatment;
- If the risk is high and the cost is comparatively low, treatment should occur;
- The most difficult area occurs between these extremes.

Risk Treatment (2)



Risk Treatment (3)

Index

Case Study: Silver Star Mine (1)

A case study involving the operations of company Silver Star Mines illustrates this risk assessment process.

- Silver Star Mines is the local operations of a large global mining company;
- It has a large IT infrastructure;
- Its network includes a variety of servers, executing a range of application software;
- It uses also applications directly related to the health and safety of those working in the mine;
- Many of these systems used to be isolated, with no network connections among them;
- In recent years, they have been connected together and connected to the companys intranet to provide better management capabilities.

Case Study: Silver Star Mine (2)

The security analyst and company management decided to adopt a **combined approach**:

- The analyst was asked to conduct a **preliminary** formal assessment of the key IT systems;
- The **context** for the risk assessment was determined: being in the mining industry sector places the company at the less risky end of the spectrum;
- SSM is part of a large organization and hence is subject to legal requirements for occupational health and safety. Thus management **decided to accept only moderate or lower risks.**

Assets Identification (1)

The analyst conducted interviews with key IT and engineering managers in the company, identifying the following key assets:

- **SCADA Network**;
- **Data integrity**;
- **Financial, Procurement and Maintenance/Production servers;**
- **Email service**.

Having determined the list of key assets, the analyst needed to identify significant threats to these assets and to specify the likelihood and consequence values.

Assets Identification (2)

SCADA Network:

- Control and monitor the core mining operations.
- Maintain the records required by law.

Data integrity:

- Data collected from different sources;
- Some of this data are required by law;
- Data on production and operational results are extremely valuable for the company.

Financial, Procurement and Maintenance/Production servers:

- Critical to the effective operation of core business area.

Email service:

- Used across all business areas.
- Greater importance given, due to the remote location of the

Level of Risk: SCADA Network

- **Threat**: unauthorized compromise of nodes by external source.
- **Existing controls**: recently additional firewall and proxy service was introduce to connect the system to the intranet.
- **Likelihood: Rare**
  - An external attack require a series of security breaches;
  - Various computer crime surveys suggest that externally sourced attacks are increasing;
  - The analyst concluded that while an attack was very unlikely, it could still occur.
- **Consequences: Major**
  - Serious consequences to the safety of mine's personnel;
  - Significant financial impact (in downtime, 10 milions per hour).
  - Breach of legal requirement.

Level of Risk: Data Integrity

- **Threat**: compromise of data from internal or external sources, even malicious.
- **Existing controls**:
  - Company's intranet is shielded by the outer firewall;
  - Policies on the input handling of data;
  - Policies on data backup from server.
- **Likelihood: Possible**
  - Overall compliance with the policies listed above is unknown.
  - Computer crime surveys indicate these kind of data as primary goal of intruder.
- **Consequences: Major**
  - Financial harm due to the confidential nature of these data.
  - Financial cost involved with the recover of data operations.
  - Legal consequences in case of personal informations disclosure.

Level of Risk: Financial and Procurement Servers

- **Threat**: any form of attack on perating systems or application they use.
- **Existing controls**:
  - Servers are placed in the company's intranet, thus are shielded by the outer firewall.
- **Likelihood: Possible**
  - Any failure in company's outer firewall could very likely result in compromise of some systems;
  - Security reports indicate that unpatched systems could be compromised in less than 15 minutes after network connection.
- **Consequences: Moderate**
  - Propotional to extent and duration of the attack;
  - Rebuild of at least a portion of the system.
  - False orders or inability to issue order.
  - Inability of use electronic found.

Level of Risk: Maintenance/Production Servers

- **Threat**: any form of attack on perating systems or application they use.
- **Existing controls**:
  - Servers are placed in the company's intranet, thus are shielded by the outer firewall.
- **Likelihood: Possible**
  - Any failure in company's outer firewall could very likely result in compromise of some systems;
  - Security reports indicate that unpatched systems could be compromised in less than 15 minutes after network connection.
- **Consequences: Minor**
  - Detrimental impact on the efficiency of operations;
  - The systems are capable to operate despite some compromise of the systems.

Level of Risk: E-Mail Service

- **Threat**: e-mailed worms and DoS attacks.
- **Existing controls**:
  - The company does filter e-mail in its Internet gateway.
- **Likelihood: Almost Certain**
  - The use of e-mail attachments could be used to compromise these systems;
  - DoS attacks against the mail gateway is very hard to defend.
- **Consequences: Major**
  - Financial costs and time to rebuild the e-mail system;
  - Inability to send or receive reports may affect the company reputation.
  - However the compromise of such system would not have a large impact on the company's operations.

Case Study: Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	Layered, firewalls and servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	Firewall, policies	Possible	Major	Extreme	2
Availability and integrity of financial system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	3
Availability and integrity of procurement system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	4
Availability and integrity of maintenance/ production system	Attacks/errors affecting system	Firewall, policies	Possible	Minor	Medium	5
Availability, integrity, and confidentiality of mail services	Attacks/errors affecting system	Firewall, ext mail gateway	Almost certain	Minor	High	6

Case Study: Conclusions

All of the resulting risk levels are above the acceptable minimum management specified as tolerable. **Hence treatment is required**:

- Management decided the first five risks should be treated by implementing suitable controls, which would reduce either the likelihood or the consequence should these risks occur. None of these risks could be accepted or avoided;
- Management decided that the risk to the SCADA network was unacceptable if there was any possibility of death, however remote;
- Responsability for the final risk to the e-mail system was found to be primarily with the parent companys IT group, which manages the external mail gateway. Hence the risk is shared with that group.