

Adatbiztonság a gazdaságinformatikában

Risk assessment

Dr. Bencsáth Boldizsár
adjunktus

BME Híradástechnikai Tanszék
bencsath@crysys.hit.bme.hu



2011. november
19.
Budapest

Risk management

- Data Security is a management problem:
 - There is no total security
 - Some risk can be acceptable
 - Budget controls what countermeasures can we afford
 - Management decides what risk do they tolerate
 - We have to formulate the “risk”

- Let's consider two companies
 - Our own university with 6 faculties, hundreds of departments. Central financial activities, dormitories.
 - A big Hungarian bank, multiple branches, office etc
- What should we protect in these companies
- At what extent
- Should we implement company wide
 - Virus protection
 - Internal firewalls between departments?
 - Filtering of incoming traffic (incoming ports, virus, etc?)
 - Filtering of outgoing traffic (e.g. spam, attacks?)
 - Ban on WIFI equipment?
 - Full disk encryption on every notebook?
 - Banning USB sticks?
 - Can we afford these steps?
 - Company wide policy on operating system and office software versions, PDF readers?
 - Company wide disaster recovery plan, regular tests, full backup?
 - Thin clients?

- We agree that the use of security tools depend about the environment we intend to introduce to.
- Besides that, the possible gains through those tools differ a lot
- Let's formulate the "Risk"

$$R = \sum_i L_i * p(L_i)$$

- R: Risk
 - L: Loss
 - p: probability
-
- The total risk of the company is the sum of the individual risks

- Based on the risk values, You can decide on the countermeasures
- Of course, this handling of risk is too simple
- Law can enforce some countermeasures / or threat is unacceptable at all (You cannot decide about)
- Some countermeasures help on more risks, or they are already implemented
- Other factors: Complexity of the risk/countermeasure, evaluation problems of the risk (the factors can only be guessed)

Likelihood

Likelihood	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years.
Low	Likely to occur one every year or less.
Medium	Likely to occur once every six months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month
Extreme	Likely to occur multiple times per day

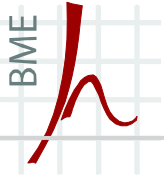
Impact Severity	Description
Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of Government information or services.
Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.

Risk determination

Likelihood of Occurrence	Impact Severity					
	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

Possible countermeasures table

Item No.	Counter-measure	Price and applicability	Helps/solves threat no.
1			
2			

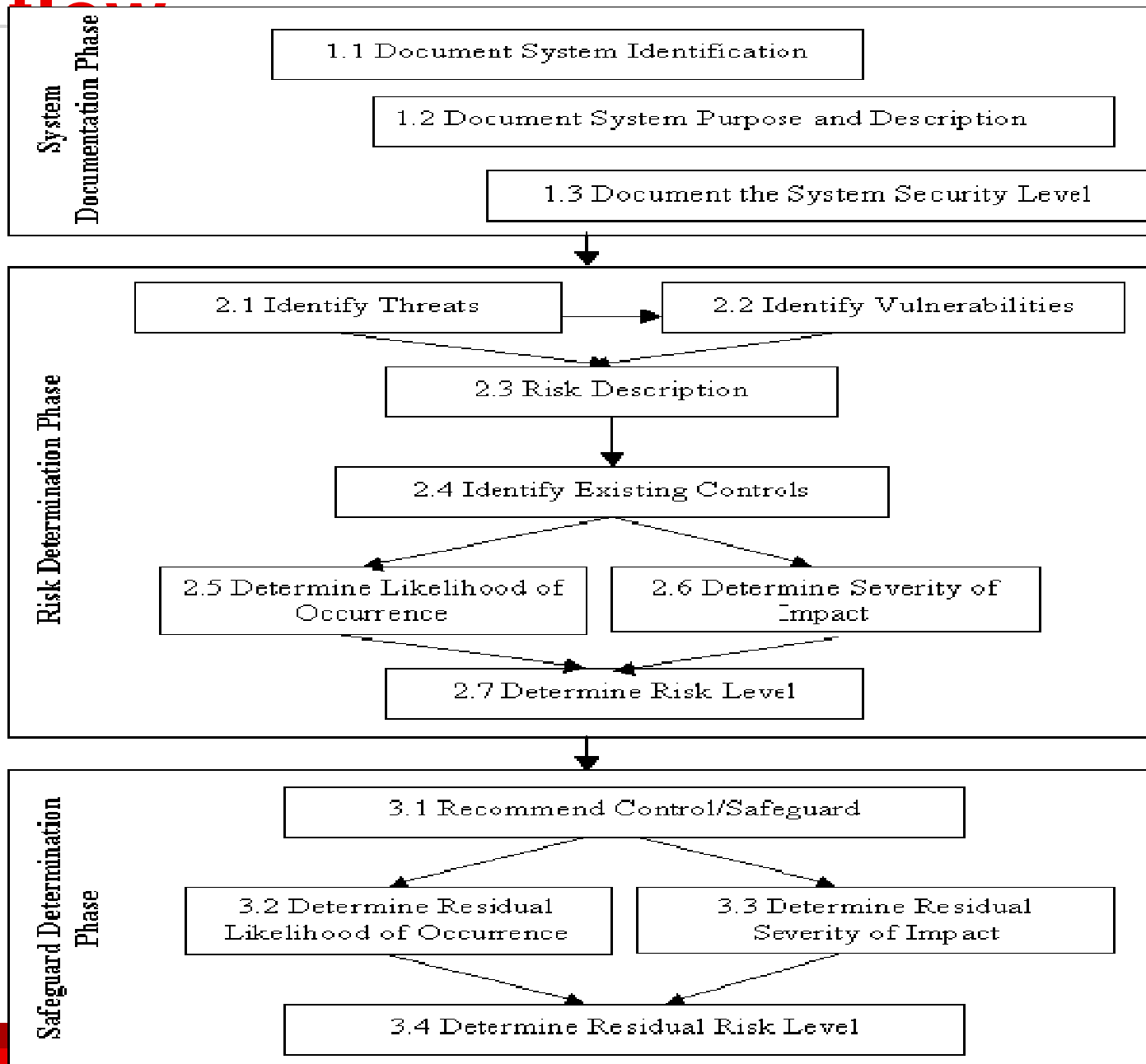


Risk determination table

Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level
1							
2							

Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level	Counter-measures/Safeguards	Remaining Risk
1									
2									

A sample risk assessment process



Sample Risk assessment chart

RISK ASSESSMENT				RISK MANAGEMENT	
Vulnerability	Risk Level	Recommended Safeguard	Residual Risk	Status of Safeguard	Updated Risk
V1: The assigned ISSO to the DSRDS GSS lacks the technical knowledge specific to this system	HIGH	Ensure the ISSO assigned responsibility to the DSRDS GSS has complete understanding of the system and receives appropriate levels of training	Low	Continuous training for the ISSO will be scheduled as training funds become available	HIGH
V2: Backup tapes are not stored off-site	HIGH	Store backup tapes off-site, as well as on-site	Low	3 cycles of weekly and daily backup tapes are stored off-site	Low

- processing or communication services that are provided by a system to give a specific kind of protection to system resources
- implement security policies -> closely related to general security objectives
- implemented by security mechanisms
- X800 (OSI security architecture) security services:
 - authentication
 - access control
 - confidentiality
 - integrity
 - non-repudiation
 - + availability is treated as a property

it's not always obvious how to achieve it!

- aims to detect masquerade
- provides assurance that a communicating entity is the one that it claims to be

peer entity authentication

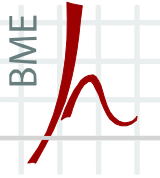
- provides for the corroboration of the identity of a peer entity in an association (logical connection)
- can be performed at the establishment of, or at times during the lifetime of the connection

data-origin authentication

- provides assurance that the source of data received in a connectionless transfer is as claimed

Access control

- prevention of unauthorized access to a resource
 - who can have access to a resource?
 - under what conditions access can occur?
 - what is allowed to do with the resource?



Confidentiality

- protection of data from unauthorized disclosure

connection confidentiality

- confidentiality protection of all data transferred via a connection

connectionless confidentiality

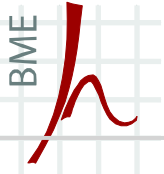
- confidentiality protection of data in a single message

selective-field confidentiality

- confidentiality protection of selective fields within a single message or messages in a connection

traffic flow confidentiality

- protection of information that might be derived from



Integrity

- aims to detect modification and replay
- provides assurance that data received are exactly as sent by the sender

connection integrity

- provides for the integrity of a stream of messages (all data on a connection)
- ensures that messages are received as sent, with no duplication, modification, insertion, deletion, reordering, or replays

connectionless integrity

- provides protection against modification of a single message
- may provide limited forms of replay detection

selective field integrity

- provides for the integrity of selective fields within a single

Non-repudiation

- provides protection against denial by one entity involved in a communication of having participated in all or part of the communication

non-repudiation of origin

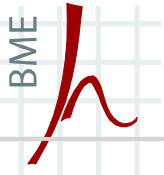
- provides proof that a message was sent by a specified party

non-repudiation of delivery

- provides proof that a message was received by a specified party

Specific security mechanisms

- encryption
 - symmetric, asymmetric
- digital signature
- access control schemes
 - access control lists, capabilities, security labels, ...
- data integrity mechanisms
 - message authentication code, sequence numbering, time stamping, cryptographic chaining
- authentication protocols
 - passwords, cryptographic techniques, biometrics
- traffic padding
- routing control
 - selection of physically secure routes
- notarization
 - e.g., time stamping, conflict resolution

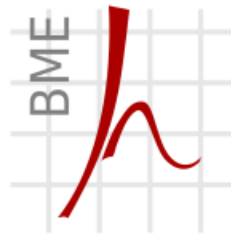


Relationship between services and mechanisms

	encryption	digital signature	access control schemes	data integrity	authentication protocols	traffic padding	routing control	notarization
peer entity authentication	✓	✓			✓			
data origin authentication	✓	✓		✓				
access control			✓					
confidentiality	✓						✓	
traffic flow confidentiality	✓					✓	✓	
data integrity	✓	✓		✓				
non-repudiation		✓						✓

Kérdések?

KÖSZÖNÖM A FIGYELMET!



Híradástechnikai Tanszék

Dr. Bencsáth Boldizsár
adjunktus

BME Híradástechnikai Tanszék
bencsath@crysys.hit.bme.hu

