

UNIVERSITY OF TRENTO

Security Engineering
MSc in Computer Science
EIT Master on Security and Privacy

Lecture 04 – Risk Assessment
Fabio Massacci

UNIVERSITY OF TRENTO

Lecture Outline

- **Introduction to Risk Assessment**
 - Risk Model
 - Assessment Approaches
 - Analysis Approaches
- **Standards for Risk Assessment**
 - ISO/IEC 27005, ISO/IEC 31000, NIST 800-30
- **“Dive” into NIST 800-30**

24/09/14 Massacci-Paci-Security Engineering ▶ 2

UNIVERSITY OF TRENTO

Introduction to Risk Assessment

UNIVERSITY OF TRENTO

Recall: Plan-Do-Check-Act Process

Plan

- Identify ISMS scope and policy
- **Identify and assess the risks**
- Select Control Objectives and Security Controls for Risk Treatment
- Formulate a Risk Treatment Plan
- Prepare a SoA

Do

- **Implement Risk Treatment Plan**
- Implement controls selected to meet control objectives

ISMS Process

Check

- **Execute Monitoring Procedures**
- Undertake Reviews
- Conduct an internal audit

Act

- **Improve Existing Controls**
- **Manage Changes**
- **Introduce New Controls**
- Reorganize Existing and New Controls

24/09/14 Massacci-Paci-Security Engineering ▶ 4

What is Risk Management?

- **Risk Assessment**
 - Identify
 - Estimate
 - Evaluate
- **Risk Mitigation**
 - Possible security controls
 - Adopt the suitable controls
- **Risk Acceptance**
 - Evaluate the residual risk
- **Risk Communication**
 - Communicate throughout the organization

24/09/14 Massacci-Paci-Security Engineering 5

Standards for Risk Management: ISO vs NIST

24/09/14 Massacci-Paci-Security Engineering 6

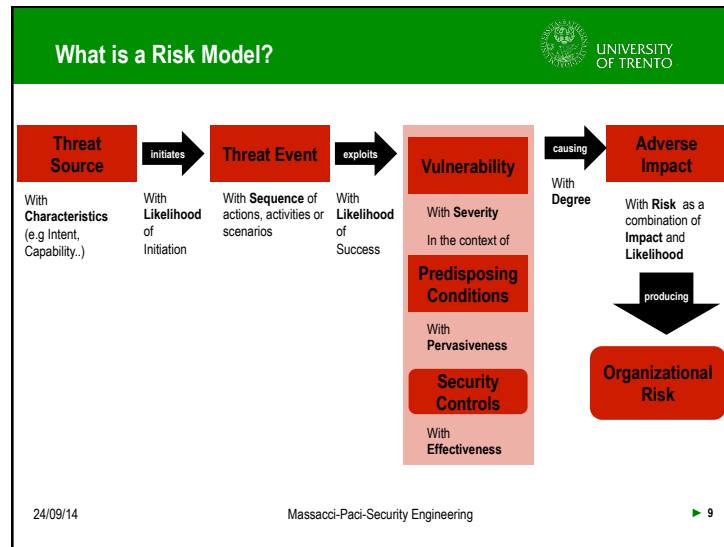
What is Risk Assessment?

- **Process to determine risks that affect organization's operations, assets, individuals, other organizations and even the nation**
- **Main steps**
 - Identifying security risks
 - Estimating security risks
 - Prioritizing security risks

24/09/14 Massacci-Paci-Security Engineering 7

What is a Risk Assessment Methodology?

24/09/14 Massacci-Paci-Security Engineering 8



- ### Threat Event, Threat Source, Threat Scenarios
- **Threat Source**
 - Entity who causes the threat
 - e.g attacker who wants to steal credit card numbers
 - **Threat Event**
 - Event or circumstance with potential adversely impact to organizational assets
 - e.g create counterfeit/spoof merchant web site
 - **Threat Scenario**
 - Set of discrete threat events that cause harm
 - E.g cross-site-scripting + phishing
- 24/09/14 Massacci-Paci-Security Engineering 10

- ### Vulnerability and Predisposing Condition
- **Vulnerability**
 - Weakness that could be exploited by a threat source
 - e.g inject arbitrary JavaScript code into the PayPal web site search function
 - **Predisposing condition**
 - Condition which affects the likelihood that a threat event results in adverse impact to organizational assets
 - e.g the web site looks trusted
 - e.g the use of a corporate network rather than a open network
- 24/09/14 Massacci-Paci-Security Engineering 11

- ### Likelihood, Impact, Risk, Uncertainty
- **Likelihood**
 - Probability that a threat event will occur
 - Probability that a threat event results in an adverse impact
 - **Adverse Impact**
 - Magnitude of the harm caused by a threat event
 - **Risk**
 - Function of Likelihood and Adverse Impact
 - **Uncertainty**
 - Imprecision/Degree of Belief/Lack of knowledge in Estimating Risk Factors
- 24/09/14 Massacci-Paci-Security Engineering 12

What is Risk Assessment?

- Aims to evaluate risk factors
- Two main approaches
 - Quantitative
 - Employ methods, principle or rules based on the use of numbers (scale 0-10)
 - Qualitative
 - Employ methods, principle or rules based on non-numerical categories or levels (e.g very low, low, moderate, high, very high)

24/09/14 Massacci-Paci-Security Engineering 13

Quantitative vs Qualitative Approach

Quantitative Approach

- Impact of cardholder data disclosure: \$ 10.000
- Likelihood of occurrence of XSS threat event : 0.80
- Risk = 10.000 x 0.80 = 8.000

Qualitative Approach

- Impact of cardholder data disclosure : High
- Likelihood of occurrence of XSS threat event: High
- Risk :

Impact/ Likelihood	Very High	High
Very High	Very High	High
High	Very High	High
Moderate	High	Moderate
Low	Moderate	Low
Very Low	Low	Low

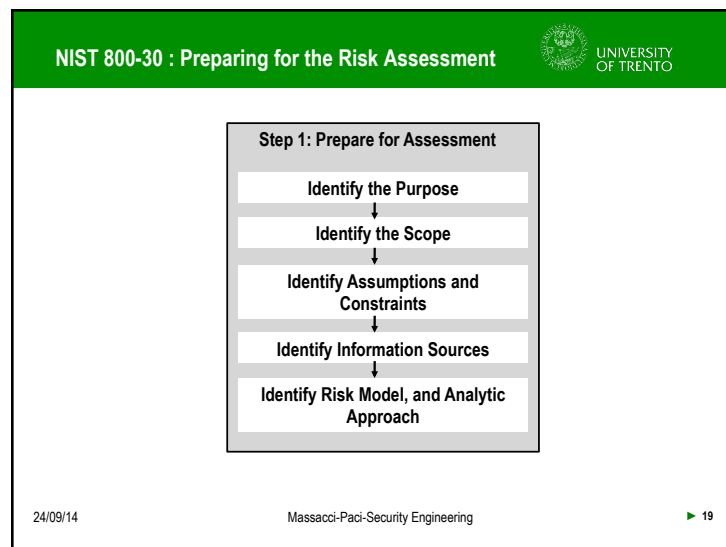
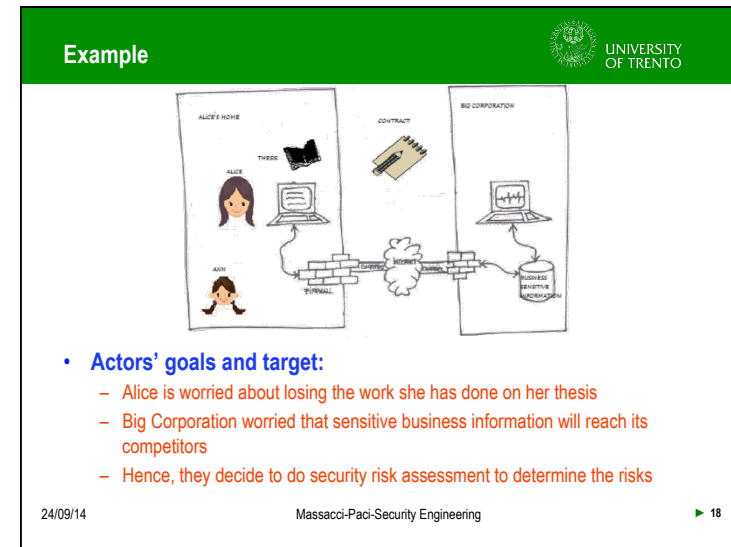
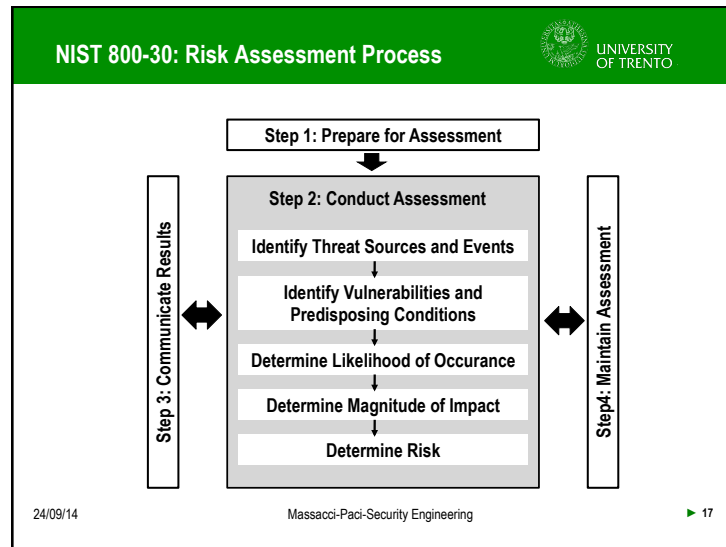
24/09/14 Massacci-Paci-Security Engineering 14

What is Risk Analysis?


- The process of identifying, assessing risks
- Possible approaches:
 - Threat-oriented
 - Asset/Impact-oriented
 - Vulnerability-oriented

24/09/14 Massacci-Paci-Security Engineering 15

NIST 800-30 standard for risk assessment



- ### NIST 800-30 : Preparing for the Risk Assessment
- **Risk Purpose**
 - Establishing a baseline assessment of risk
 - **Decision Supported**
 - Selection of Controls
 - **Assumptions and Constraints**
 - All possible threat sources and events (that we consider)
 - **Risk Model and Analytical Approach**
 - Threat Oriented
 - Qualitative
- 24/09/14 Massacci-Paci-Security Engineering ▶ 20

NIST 800-30 : Conduct Assessment 

Step 2: Conduct Assessment

Identify Threat Sources and Events
↓

Identify Vulnerabilities and Predisposing Conditions
↓

Determine Likelihood of Occurance
↓

Determine Magnitude of Impact
↓


Determine Risk

24/09/14 Massacci-Paci-Security Engineering ▶ 21

Conduct Assessment: Identify Threats 


- **Identify threat sources**
 - Identify threat sources relevant for the organization
 - Assess their intent, capability and target
- **Identify threat events**
 - Determine source information to identify threats
 - Determine threats events relevant to conduct the assessment
 - Identify threat sources that could initiate the events

24/09/14 Massacci-Paci-Security Engineering ▶ 22

Conduct Assessment: Identify Threats 


Threat Source	Threat Event
Alice	Install a malware on her laptop
Outsider	Conduct SQL Injection attack to BC portal

24/09/14 Massacci-Paci-Security Engineering ▶ 23

Conduct Assessment : Identify Vulnerabilities 


- **Identify vulnerabilities using organization-defined information sources**
- **Assess the severity of identified vulnerabilities**
- **Identify predisposing conditions**
- **Assess the pervasiveness of predisposing conditions**

24/09/14 Massacci-Paci-Security Engineering ▶ 24

Conduct Assessment : Identify Vulnerabilities  UNIVERSITY OF TRENTO


Threat Source	Threat Event	Vulnerability	Predisposing Condition
Alice	Install Malware	No Anti Virus Installed	N/A
Outsider	SQL Injection Attack	No Interpreter Input Validation	N/A

24/09/14 Massacci-Paci-Security Engineering ▶ 25

Conduct Assessment: Determine Likelihood (1)  UNIVERSITY OF TRENTO

- **Determine Likelihood of Occurance**
 1. **Determine Likelihood of Threat Event Initiation**
 - Investigate Threat Source Characteristics
 2. **Determine Likelihood of Threat Event Resulting In Adverse Impact**
 - Investigate Vulnerabilities and Predisposing Conditions
 3. **Compute Overall Likelihood as combination of the two above**
 - Take Max or Min of the two
 - Consider Likelihood of Initiation
 - Consider Likelihood of Impact
 - Average of the two


24/09/14 Massacci-Paci-Security Engineering ▶ 26

Conduct Assessment: Determine Likelihood (2)  UNIVERSITY OF TRENTO

- **Likelihood of Threat Initiation Scale**

Qualitative Values	Description
Very High	Adversary is almost certain to initiate the threat
High	Adversary is highly likely to initiate the threat
Moderate	Adversary is somewhat likely to initiate the threat
Low	Adversary is unlikely to initiate the threat
Very Low	Adversary is highly unlikely to initiate the threat


24/09/14 Massacci-Paci-Security Engineering ▶ 27

Conduct Assessment: Determine Likelihood (3)  UNIVERSITY OF TRENTO

- **Likelihood of Adverse Impact Scale**

Qualitative Values	Description
Very High	It is almost certain to have adverse impacts
High	It is highly likely to have adverse impacts
Moderate	It is somewhat likely to have adverse impacts
Low	It is unlikely to have adverse impacts
Very Low	It is highly unlikely to have adverse impacts


24/09/14 Massacci-Paci-Security Engineering ▶ 28

Conduct Assessment: Determine Likelihood (4)  UNIVERSITY OF TRENTO

Likelihood of Impact/ Likelihood of Initiation	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low


Threat Source	Threat Event	Likelihood of Initiation	Likelihood of Impact
Alice	Install Malware	Moderate	High
Outsider	SQL Injection Attack	Very High	Very High

24/09/14 Massacci-Paci-Security Engineering 29

Conduct Assessment: Determine Impact (1)  UNIVERSITY OF TRENTO

- **Identify possible adverse impacts and affected assets**
 - Characteristics of threat sources
 - Vulnerabilities and predisposing conditions
 - Susceptibility given implemented security controls
- **Possible adverse impacts**
 - Harm to operations
 - Harm to assets
 - Harm to individuals
 - Harm to other organization
 - Harm to the nation


24/09/14 Massacci-Paci-Security Engineering 30

Conduct Assessment: Determine Impact (2)  UNIVERSITY OF TRENTO

- **Impact Assessment Scale**


Qualitative Values	Description
Very High	The threat event could be expected to have multiple severe or catastrophic adverse effects
High	The threat event could be expected to have severe or catastrophic adverse effects
Moderate	The threat event could be expected to have serious adverse effects
Low	The threat event could be expected to have limited adverse effects
Very Low	The threat event could be expected to have negligible adverse effects

24/09/14 Massacci-Paci-Security Engineering 31


Conduct Assessment: Determine Impact (3)  UNIVERSITY OF TRENTO


Threat Source	Threat Event	Impact
Alice	Install Malware	Moderate
Outsider	SQL Injection	Very High

24/09/14 Massacci-Paci-Security Engineering 32

Conduct Assessment: Determine Risk (1) 


- **Identify Risks as Combination of**
 - Likelihood of Occurance and
 - Impact
- **Order identified threat events based on the associated risk level**
 - Highest Risks on Top of the list
- **Prioritize threats with risks at the same level**


24/09/14 Massacci-Paci-Security Engineering  33

Conduct Assessment: Determine Risk (2) 


Impact/ Likelihood	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low


Threat Source	Threat Event	Likelihood of Occurance	Impact
Alice	Install Malware	Moderate	Moderate
Outsider	SQL Injection Attack	Very High	Very High

24/09/14 Massacci-Paci-Security Engineering  34


NIST 800-30 : Communicate Results 


- **Determine the appropriate method to communicate risk results**
 - Executive briefing, risk assessment report....
- **Share risk-related information produced during the assessment**
- **Report**
 - Purpose
 - Scope
 - Assumptions and Constraints
 - Risk Tolerance Inputs
 - Risk Model, Assessment and Analysis Approaches
 - List of Prioritized Threat Events based on their risk level

24/09/14 Massacci-Paci-Security Engineering  35


NIST 800-30 : Maintain Assessment 

- **Monitor Risk Factors**
 - Identify risk-impacting changes
 - Determine changes in the effectiveness of security controls
- **Update Risk Assessment**
 - Revisit purpose, scope, assumptions, and constraints
 - Lead to subsequent risk assessment
- **Communicate Results**

24/09/14 Massacci-Paci-Security Engineering  36

 UNIVERSITY OF TRENTO


**What you have to do for the assignments:
Your risk management process**

 UNIVERSITY OF TRENTO

Risk Management Process on ...

- **Risk Assessment**
 - Identify threat sources and events using CORAS or SecRAM
 - Focus on threat sources and events specific for
 - Define likelihood and impact scales
- **Risk Mitigation**
 - Identify Security Controls
 - Use NIST 800-53 and ... as starting point
- **Risk Acceptance**
 - Evaluate residual risk
- **Risk Communication**
 - Write the report using the template on webpage

24/09/14 Massacci-Paci-Security Engineering ▶ 38

 UNIVERSITY OF TRENTO

Suggested Readings

- Chapter 16. Stallings, Brown. Computer Security
- NIST SP 800-30 – Guide for Conducting Risk Assesments. Freely Available from NIST web site
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations. Freely Available from NIST web site

24/09/14 Massacci-Paci-Security Engineering ▶ 39