CHƯƠNG 03

QUI TRÌNH ĐÁNH GIÁ RỦI RO (RISK ASSESSMENT)

10/2/2021

ThS.Nguyễn Duy
duyn@uit.edu.vn

Nội Dung

- Thu thập dữ liệu
- Phân tích dữ liệu
- Đánh giá rủi ro (risk assessment)
- Phân cấp rủi ro và giải quyết rủi ro (Risk Prioritization and treatment)

Nội Dung

- **Thu thập dữ liệu**
- Phân tích dữ liệu
- Đánh giá rủi ro (risk assessment)
- Phân cấp rủi ro và giải quyết rủi ro (Risk Prioritization and treatment)

Thu thập dữ liệu

- Cơ chế thu thập dữ liệu
- Những tài liệu yêu cầu
- Tài liệu khảo sát

Thu thập dữ liệu
Cơ chế thu thập dữ liệu - Collector

- Những loại dữ liệu cần được thu thập:
  - System profiles
  - Control profiles
  - Audit report
  - Vulnerability assessments
  - Various information security event and metrics.
- Phương pháp thu thập:
  - Yêu cầu tài liệu
  - Khảo sát
  - Phỏng vấn

Thu thập dữ liệu
Cơ chế thu thập dữ liệu - Container

- Container là những tài nguyên mà ở đó dữ liệu thu thập được lưu trữ.
  - Ví dụ: Table of Database, Spreadsheet,…
- 4 container phổ biến:
  - Finding
  - Assets
  - Risk
  - Reference data

Thu thập dữ liệu
Cơ chế thu thập dữ liệu - Container

- Finding
  - Finding Statement.
  - Description.
  - Asset.
  - Source.
  - Risk Rating.
  - Status.
  - System.

Thu thập dữ liệu

Cơ chế thu thập dữ liệu - Container

Finding State-ment	Description	Asset	Source	Risk Rating	Status	System
Phishing incidents	A review of security incident data collected over the past year shows that a large number of the incidents documented were related to some form of phishing or social engineering attack. Either a user provided their user name and creden-tials or clicked on a malicious link or attachment	Users	Security Incident Metrics collected by ISO	High—was considered an incident	No action taken	None but attempts were through the email system

Thu thập dữ liệu
Cơ chế thu thập dữ liệu - Container

- Assets
  - Asset Name.
  - Asset Classification.
  - Control Information (multiple sub-elements).

Thu thập dữ liệu
Cơ chế thu thập dữ liệu - Container

- Risk
  - Asset/Application
  - Threat.
  - Impact
  - Likelihood
  - Risk Score.

Application: Hospital Information System					
Threat (Agent and Action)		**Vulnerability**	**Impact Score**	**Likelihood Score**	**Risk Score**
Users	Eavesdrop-ping and Interception of data	Lack of trans-mission encryp-tion leading to interception of unencrypted data	5	2	10

Thu thập dữ liệu
Cơ chế thu thập dữ liệu - Container

- Reference data
  - Threat Catalog.
  - Document Request Lists.
  - Data Sources.
  - Asset Inventory.
  - Interview Notes.

EXECUTIVE INTERVIEWS

- Chief Executive Officer
- Chief Information Officer
- Chief Technology Officer
- Chief Operations Officer
- Chief Financial Officer
- Chief Information Security Officer
- Chief Privacy Officer
- Chief Risk and Compliance Officer or Risk Management Director
- Internal Audit Director
- Vice Presidents and/or Directors of various departments

Thu thập dữ liệu
Những tài liệu yêu cầu

- Previous Information Security Risk Assessment
- Previous IT Risk Assessment
- Previous Audit reports
- Previous Regulatory or Framework Driven Assessments
- Previous Penetration Testing Reports
- Previous Vulnerability Assessments
- Current Security Policy, Standards and Procedures

Thu thập dữ liệu
Những tài liệu yêu cầu – cont.

- Disaster Recovery and Business Continggency Plans
- Request a copy of the BIA
- Asset Inventories
- IT and Information Security Metrics
- Facilities Security Plan
- Organizational Chart and contact list
- Security Program, Plans and Roadmap
- Vendor Security Accrediations
- Hardening Guidelines and Checklist

Thu thập dữ liệu
Tài liệu khảo sát

- System name
- System description
- Vendor
- Platform
- System owner
- System steward
- Technical contact
- Data Classification
- Accessibility

Thu thập dữ liệu
Tài liệu khảo sát

- Location
- Data Flow
- Users
- User Profile
- Security Incident
- Security Testing
- Business impact

Nội Dung

- Thu thập dữ liệu
- **Phân tích dữ liệu**
- Đánh giá rủi ro (risk assessment)
- Phân cấp rủi ro và giải quyết rủi ro (Risk Prioritization and treatment)

Phân tích dữ liệu

- Phân tích và thiết kế tác động
- Phân tích và thiết kế cơ chế kiểm soát
- Phân tích và thiết kế xác suất có thể xảy ra

Phân tích dữ liệu
Phân tích và thiết kế tác động

- Confidentiality

Table 4.3 Sample Confidentiality Determination Matrix

Confidentiality Determination Matrix		
Score	**Description**	**Criteria**
5	VERY HIGH	Data Classification = Confidential with an additional classification of Legally Privileged or Regulated Data
4	HIGH	Data Classification = Confidential
3	MEDIUM	Data Classification = Internal
2	LOW	Data Classification = Public
1	VERY LOW	Unclassified

Phân tích dữ liệu
Phân tích và thiết kế tác động - tt

Table 4.4 Sample Confidentiality Determination Matrix

Confidentiality Determination Matrix		
Score	**Description**	**Criteria**
5	VERY HIGH	• Data Classification = Confidential with an additional classification of Legally Privileged or Regulated Data AND • Number of Records = HIGH
4	HIGH	• Data Classification = Confidential with an additional classification of Legally Privileged or Regulated Data AND • Number of Records = MEDIUM OR LOW
3	MEDIUM	• Data Classification = Confidential AND • Number of Records = HIGH
2	LOW	• Data Classification = Confidential AND • Number of Records = MEDIUM OR LOW
1	VERY LOW	• Data Classification = All Non Confidential

Phân tích dữ liệu
Phân tích và thiết kế tác động

- Integrity

Table 4.5 Sample Integrity Determination Matrix

Integrity Determination Matrix		
Score	**Description**	**Criteria**
5	VERY HIGH	• Business Critical = High • Financially Material = YES
4	HIGH	• Business Critical = Moderate OR Low • Financially Material = YES
3	MEDIUM	• Business Critical = Moderate • Financially Material = NO
2	LOW	• Business Critical = NO • Financially Material = NO
1	VERY LOW	• Not Applicable

Phân tích dữ liệu
Phân tích và thiết kế tác động

Table 4.5 Sample Integrity Determination Matrix

Integrity Determination Matrix		
Score	**Description**	**Criteria**
5	VERY HIGH	• Business Critical = High • Financially Material = YES
4	HIGH	• Business Critical = Moderate OR Low • Financially Material = YES
3	MEDIUM	• Business Critical = Moderate • Financially Material = NO
2	LOW	• Business Critical = NO • Financially Material = NO
1	VERY LOW	• Not Applicable

Phân tích dữ liệu
Phân tích và thiết kế tác động

- Availability

Table 4.7 Sample Availability Determination Matrix

Availability Determination Matrix		
Score	**Description**	**Criteria**
5	VERY HIGH	• Business Critical = YES • Number of Users = High
4	HIGH	• Business Critical = YES • Number of Users = Medium OR Low
3	MEDIUM	• Business Critical = NO • Number of Users = High
2	LOW	• Business Critical = NO • Number of Users = Medium
1	VERY LOW	• Business Critical = NO • Number of Users = Low

Table 4.8 Sample Assignment of CIA Impact Scores

Application: Hospital Information System						
Threat (Agent and Action)		**Vulnerability**	**C**	**I**	**A**	**Impact Score**
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	5	0	0	5
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	5	5	0	5
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	0	5	0	5
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	0	5	0	5
Non-Specific, Natural	Loss of power	Lack of redundant power supply	0	0	5	5
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	0	0	5	5

Phân tích và thiết kế cơ chế kiểm soát

- Data Protection
- Patch Management
- Complex Passwords
- Vulnerability Management
- Security Configuration
- Authentication Controls
- IDS/IPS Monitoring
- User Provisioning
- Transmission Encryption
- AV/HIPS
- Account Management
- Security Isolation
- Logging and Monitoring
- Storage Encryption
- Enterprise Backup
- Redundancy and Failover
- BCP/DR
- Change Control
- Security Awareness

Table 4.10 Control Level Table

Control Level			
Score	**Reverse**	**Description**	**Criteria**
5	.2	VERY STRONG	Control provides very strong protection against the threat. Threat being successful in leveraging the vulnerability is highly unlikely. Effectiveness of the control is being reviewed constantly. Process is defined and documented. Controls are consistently enforced. Performance is monitored.
4	.4	STRONG	Control provides strong protection against the threat leveraging the vulnerability. Performance of the control is enforced. Process is defined and documented. Controls are consistently enforced.
3	.6	MODERATE	Control provides protection against the threat leveraging the vulnerability but may have exceptions. Control is enforced but not consistently or incorrectly.
2	.8	WEAK	Controls provide some protection against threat leveraging the vulnerability but mostly ineffective. Formal process may exist but control may not be enforced.
1	1	VERY WEAK	No control or control provides protection against the threat leveraging the vulnerability. Formal process and enforcement of controls are ad hoc or non-existent.

Table 4.12 Sample Control Analysis

Application: Hospital Information System				
Threat (Agent and Action)		**Vulnerability**	**Controls**	**Controls Score**
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	Transmission Encryption	4
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	Complex Passwords	4
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	Generic Account Use Policies	3
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	Logging and Monitoring Controls	3
Non-Specific, Natural	Loss of power	Lack of redundant power supply	Alternate Power Supply	4
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	Physical and Environmental Controls	4

Phân tích và thiết kế xác suất có thể xảy ra

- Exposure
  - Exposure is the predisposition of the system to the threat based on environmental factors.
  - For example, if an asset is exposed to the Internet, then the probability of system intrusions due to external intruders increases.

Table 4.15 Computing for Exposure

Application: Hospital Information System						
Threat (Agent and Action)		**Vulnerability**	**Exposure**	**Frequency**	**Control**	**Likelihood**
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	3			
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	3			
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	5			
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	5			
Non-Specific, Natural	Loss of power	Lack of redundant power supply	5			
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	2			

Table 4.16 Sample Exposure Determination

Exposure Determination Matrix for Eavesdropping and Interception of data		
Score	**Description**	**Criteria**
5	VERY LIKELY	Previous incidents or attempted eavesdropping attacks and weaknesses have been documented
4	LIKELY	System transfers sensitive data over the Internet (any number or records)
3	MODERATE	System transfers a large number of sensitive data within the internal network
2	UNLIKELY	System transfers a low number of sensitive data within the internal network
1	VERY UNLIKELY	No data is transferred

Table 4.17 Sample Exposure Determination

Exposure Determination Matrix for System Intrusion and Unauthorized System Access		
Score	**Description**	**Criteria**
5	VERY LIKELY	Previous compromises or attempts have been detected
4	LIKELY	System is Internet accessible
3	MODERATE	System is remotely accessible (e.g. via VPN)
2	UNLIKELY	System is accessible only through the internal network
1	VERY UNLIKELY	Anything that does not fall into the UNLIKELY criteria (e.g. a standalone system without network access)

Table 4.23 Adding Frequency Scores

Application: Hospital Information System						
Threat (Agent and Action)		**Vulnerability**	**Exposure**	**Frequency**	**Control**	**Likelihood**
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	3	3		
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	3	5		
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	5	1		
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	5	2		
Non-Specific, Natural	Loss of power	Lack of redundant power supply	5	2		
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	2	1		

Table 4.22 Frequency Matrix

Frequency Matrix		
Score	**Description**	**Criteria**
5	VERY LIKELY	Could happen on a daily basis
4	LIKELY	Could happen on a weekly basis
3	MODERATE	Could happen on a monthly basis
2	UNLIKELY	Could happen within 1 year
1	VERY UNLIKELY	Could happen within 5 years

Table 4.24 Adding Control Scores

Application: Hospital Information System						
Threat (Agent and Action)		**Vulnerability**	**Exposure**	**Frequency**	**Control**	**Likelihood**
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	3	3	4	
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	3	5	4	
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	5	1	3	
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	5	2	3	
Non-Specific, Natural	Loss of power	Lack of redundant power supply	5	2	4	
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	2	1	4	

Table 4.26 Sample Computation of Likelihood

Application: Hospital Information System						
Threat (Agent and Action)		**Vulnerability**	**Exposure**	**Frequency**	**Control**	**Likelihood**
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	3	3	4 (.4)	1.2
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	3	5	4 (.4)	1.6
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	5	1	3 (.6)	1.8
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	5	2	3 (.6)	2.1
Non-Specific, Natural	Loss of power	Lack of redundant power supply	5	2	4 (.4)	1.4
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	2	1	4 (.4)	.6

Table 4.33 Sample Risk Score

Application: Hospital Information System					
Threat (Agent and Action)		**Vulnerability**	**Impact Score**	**Likelihood Score**	**Risk Score**
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	5	2	10
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	5	2	10
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	5	2	10
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	5	3	15
Non-Specific, Natural	Loss of power	Lack of redundant power supply	5	2	10
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	5	1	5

Nội Dung

- Thu thập dữ liệu
- Phân tích dữ liệu
- **Đánh giá rủi ro (risk assessment)**
- Phân cấp rủi ro và giải quyết rủi ro (Risk Prioritization and treatment)

Application	Risk Rank
HIS	60
HR Payroll	50
Cardio Research DB	47
Email	46
Imaging	45

Email System

Description: Microsoft Exchange used by the hospital for internal and external email.

Threat Agent	Threat Action	Vulnerability	Impact	Likelihood	Risk Score	Risk Classification
Users	Eavesdropping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	5	3	15	High
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthorized system access	Possible Weak Passwords due to lack of password complexity controls	5	2	10	Moderate
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	3	2	6	Moderate
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	3	3	9	Moderate
Non-Specific, Natural	Loss of power	Lack of redundant power supply	3	1	3	Low
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	3	1	3	Low
Total					46	

Imaging System

Description: The hospitals primary radiology imaging application.

Threat Agent	Threat Action	Vulnerability	Impact	Likelihood	Risk Score	Risk Classification
Users	Eavesdrop-ping and Interception of data	Lack of transmission encryption leading to interception of unencrypted data	5	3	15	High
External Intruders, Malicious Insiders, Malicious Code	System intrusion and unauthor-ized system access	Possible Weak Passwords due to lack of password complexity controls	5	2	10	Moderate
Users	Denial of user actions or activity	Untraceable user actions due to generic accounts	5	1	5	Moderate
Malicious Insider, Users	Unchecked data alteration	Lack of logging and monitoring controls	5	1	5	Moderate
Non-Specific, Natural	Loss of power	Lack of redun-dant power supply	5	1	5	Moderate
Natural	Equipment damage or destruction due to natural causes (fire, water, etc.)	Lack of environmental controls	5	1	5	Moderate
Total					45	

Nội Dung

- Thu thập dữ liệu
- Phân tích dữ liệu
- Đánh giá rủi ro (risk assessment)
- **Phân cấp rủi ro và giải quyết rủi ro (Risk Prioritization and treatment)**

	Likelihood					
Impact		1	2	3	4	5
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Area	Risk Classificatio
Black	High Risk
Grey	Moderate Risk
White	Low Risk