CYBR3000

Qualitative Security Risk Assessment and Management

Dr Dan Kim

Associate Professor in Cybersecurity,
School of EECS
The University of Queensland, Australia
Homepage: https://researchers.uq.edu.au/researcher/23703

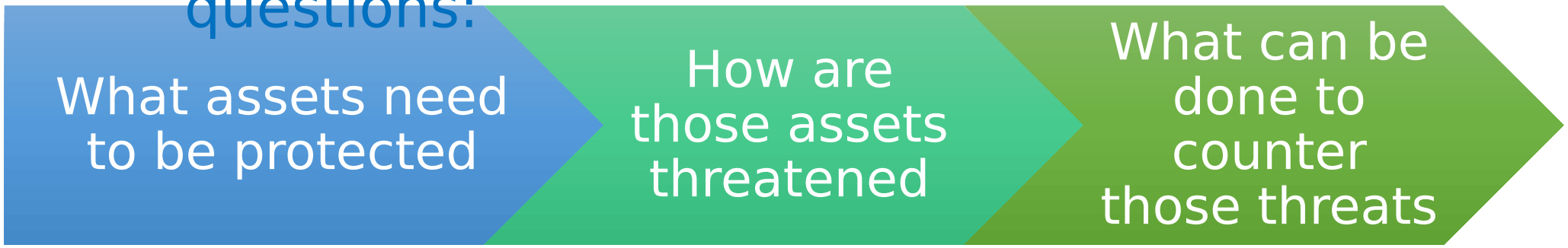
Learning objectives

- At the end of this lecture, you will be able to understand/explain
  - Security management overview
  - Steps
  - Risk assessment method
  - A few examples

Security Management Overview

- Ensures that *critical* assets are sufficiently protected in a cost-effective manner
- Security risk assessment is needed for each asset in the organization that requires protection
- Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

Formal process of answering the questions:



5 Steps


1. Asset Identification
2. Threat Identification
3. Vulnerability Identification
4. Analyze Risks
5. Analyze Existing Controls

1. Asset Identification

- Identify assets to examine
- Draw on expertise of people in relevant areas of organization to identify key assets
  - Identify and interview such personnel

Asset

- "anything which needs to be protected" has value to organization to meet its objectives tangible or intangible whose compromise or loss would seriously impact the operation of the organization

2. Threat Identification

3. Vulnerability Identification

- Identify exploitable flaws or weaknesses in organization’s 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

4. Analyze Risks

- Specify likelihood of occurrence of each identified threat to asset given existing controls

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as "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 or later.

- Specify consequence (rating: consequence) should threat occur
  - 1: insignificant, 2: minor, 3: moderate, 4: major, 5: catastrophic, 6: doomsday
- Derive overall risk rating for each threat
  - Risk = probability threat occurs x cost to organization (i.e. impact wrt CIA)
- In general, hard to determine accurate probabilities and realistic cost consequences
- Use qualitative, not quantitative, ratings

4. Analyze Risks (cont.)

- Derive overall risk rating for each threat

	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 are 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 are 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.

- In general, hard to determine accurate probabilities and realistic cost consequences; Use qualitative, not quantitative, ratings

5. Analyze Existing Controls

- Existing controls used to attempt to minimize threats need to be identified
- Security controls (see the page 19) include:
  - Management
  - Operational
  - Technical processes and procedures

- Use checklists of existing controls and interview key organizational staff to solicit information

Examples

Asset	Threat/ vulnerability	Likelihood	Consequence	Existing control(s)	Level of risk	Risk priority
Internet router	Outside attacker’s password cracking	possible	moderate	Password challenge	high	1
Data center	Accidental fire or flood	unlikely	major	None (no disaster recovery plan)	high	2
Laptop used by staff	Malware infection via phishing email	Likely	Moderate	Antivirus software, staff training	Medium	3
Cloud storage service	Unauthorized access due to weak API security	Possible	Major	API key rotation, access logging	High	4
Office building	Physical break-in	Unlikely	Moderate	Security cameras, alarm system	Low	5

Examples 2

Asset	**Threat/Vulnerability**	**Likelihood**	**Consequence**	**Existing Control(s)**	**Level of Risk**	Priority?
Smartphone	Loss or theft leading to data breach	Possible	Major	Device encryption, remote wipe capability	High	
Smart speaker	Unauthorized access via voice commands	Unlikely	Moderate	Voice recognition, limited access to sensitive data	Medium	
Laptop (AI dev)	Unauthorized access via unattended session	Likely	Major	Auto-lock, biometric login	High	
Cloud notebook	Data leakage through misconfigured permissions	Possible	Major	Access control policies, audit logs	High	
External drive	Malware infection from unverified sources	Likely	Moderate	Endpoint protection, restricted USB access	Medium	

References

- Stalling and Brown Chap 14 & 15.
- Other references are on the slides.