Overview of typical problems

SESAR SECRAM EXPERIENCE OF TWO EXERCISES

CYBER SECURITY RISK ASSESSMENT COURSE – FALL

Step 1.1: Primary Assets Identification

SecRAM definition

Primary Asset is an intangible function, service, process or information that are part of the ATM system within the scope of the project and has value to the system.

List of problems

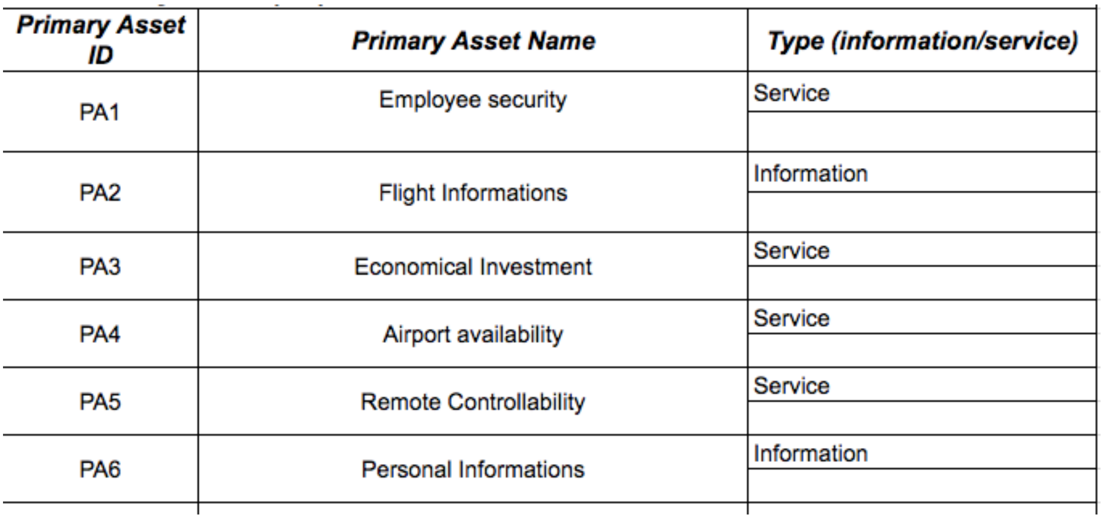
Exercise 1:

1. Security/safety in PA name (39% of works)
2. Generic PAs, e.g. Efficient, Privacy, Data (19%)
3. PAs Economic Investment, Mobility, Reputation (6%)
4. PAs like “ATS work correctly for all airport of interest” (1 work)

Exercise 2:

1. Security/safety in PA name (43% of works)
2. Generic PAs, e.g. Efficient, Privacy, Data (18%)
3. PAs Economic Investment (14%)
4. PAs like “ATS work correctly for all airport of interest” (1 work)
5. “Availability of flighting service to customers” (1 work)

Not good example



Primary Asset ID	Primary Asset Name	Type (information/service)
PA1	Employee security	Service
PA2	Flight Informations	Information
PA3	Economical Investment	Service
PA4	Airport availability	Service
PA5	Remote Controllability	Service
PA6	Personal Informations	Information

Better example for Exercise 2

Primary Asset ID	Primary Asset Name	Type (information/service)
PA1	Visualization sensors data	Information
PA2	Airport sound sensors data	Information
PA3	Visual/Non-visual navigation aid sensors data	Information
PA4	Remote control of signalling lamps system and alarm system	Service

Step 1.2: Impact assessment

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

List of problems

Exercise 1:

1. Poor impact assessment (26%)
2. No justifications (16%)
3. Generic or poor justification (16%)
4. Incomplete assessment (10%)
5. Confidentiality is not evaluated (1 work)

Exercise 2:

1. Poor impact assessment (32%)
2. Confidentiality is not evaluated (21%)
3. Problem with impact assessment and justification of PA like Safety/Security of something (21%)
4. No justifications (18%)
5. Generic or poor justification (18%)
6. Incomplete assessment (1 work)

Step 2: Supporting Assets identification

SecRAM definition

Supporting Assets are entities which enable the primary assets. Supporting assets possess the vulnerabilities that are exploitable by threats aiming to impair primary assets.

List of problems

Exercise 1:

1. SAs are out of scope (52%)
2. Not all SAs related to the focus of the exercise are included (10%)
3. Generic SAs (6%)
   - “Connections” or “Network Security”
4. Data as SA (6%)
5. Some SAs are unclear (1 work)
   - “Remote tower modules”

Exercise 2:

1. Some SAs are unclear (25%)
   - “Communication/computer system”, “New signaling lamp”, “New aids systems”, “Binoculars”
2. SAs are out of scope (18%)
3. Data as SA (7%) Links between SAs and PAs are unclear or no link provided (15%)
4. Generic SAs (6%)
   - “System Security” or “Physical Security”

Setp 3: Vulnerabilities & Threat Scenarios Evaluation

SecRAM definitions

Vulnerability is a security weakness of an asset that can be exploited by an attacker via a threat.

Threat is the potential cause of an unwanted incident which may result in an impact on the OFA.

A **threat scenario** is a combination of a threat over a supporting asset within the considered environment

List of problems

Exercise 1:

1. Generic threats (39%) and/or vulnerabilities (10%)
2. Impact evaluation problems (29%)
3. Unclear threats and/or vulnerabilities (23%)
4. Threat is not applicable to SA (6%)
5. Misunderstanding of threats and vulnerabilities (2-3 works)

Exercise 2:

1. Impact evaluation problems (32%)
2. Unclear threats and/or vulnerabilities (21%)
3. Threat is not applicable to SA (14%)
4. Generic threats (11%)
5. Misunderstanding of threats and vulnerabilities (2-3 works)

Step 5: Security Controls

SecRAM definition

Security Controls are means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.

List of problems

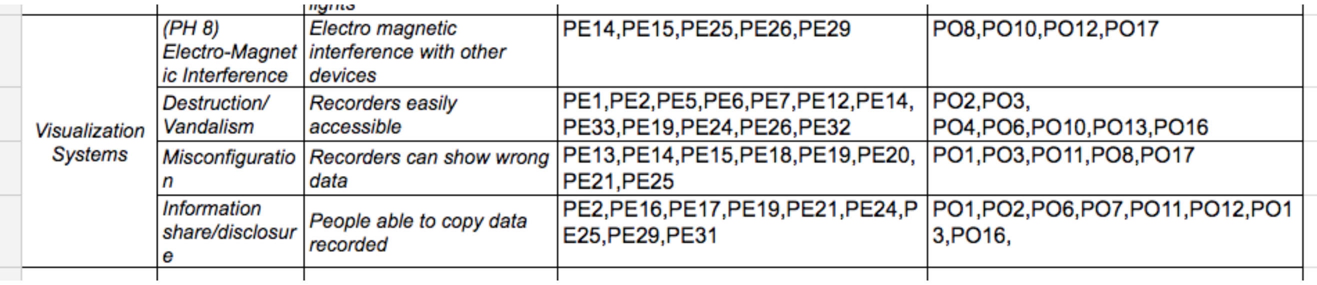
Exercise 1:

1. Lack of description/motivation behind selected controls (most of works)
2. Generic/unclear/not specific controls (32%)
3. Pre-controls do not prevent threats (13%)
4. Inapplicable controls (6%)
5. Limited selection of controls (one work)

Exercise 2:

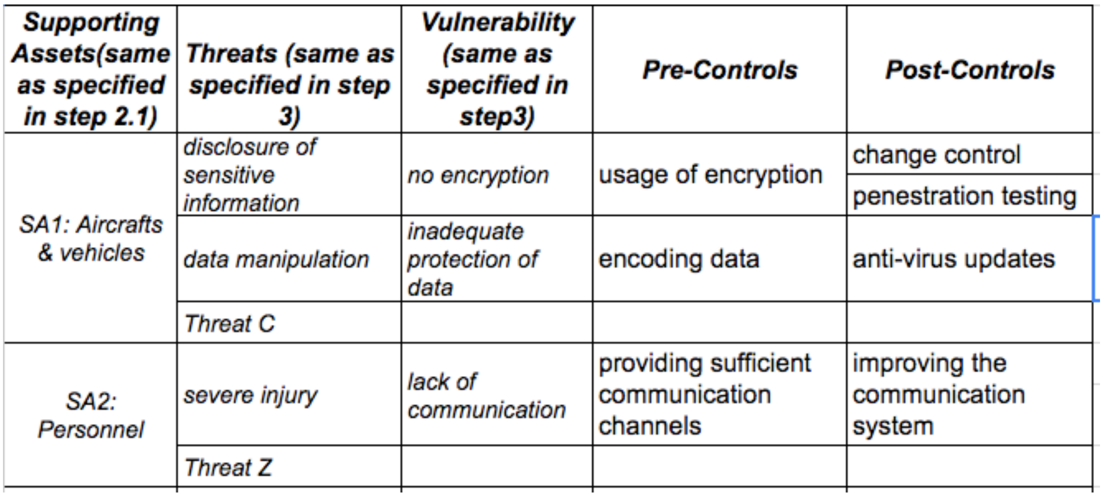
1. Lack of description/motivation behind selected controls (most of works)
2. Generic/unclear/not specific controls (29%)
3. Inapplicable controls (21%)
4. Pre-controls do not prevent threats (11%)
5. Limited selection of controls (7%)

Bad examples(1/2)



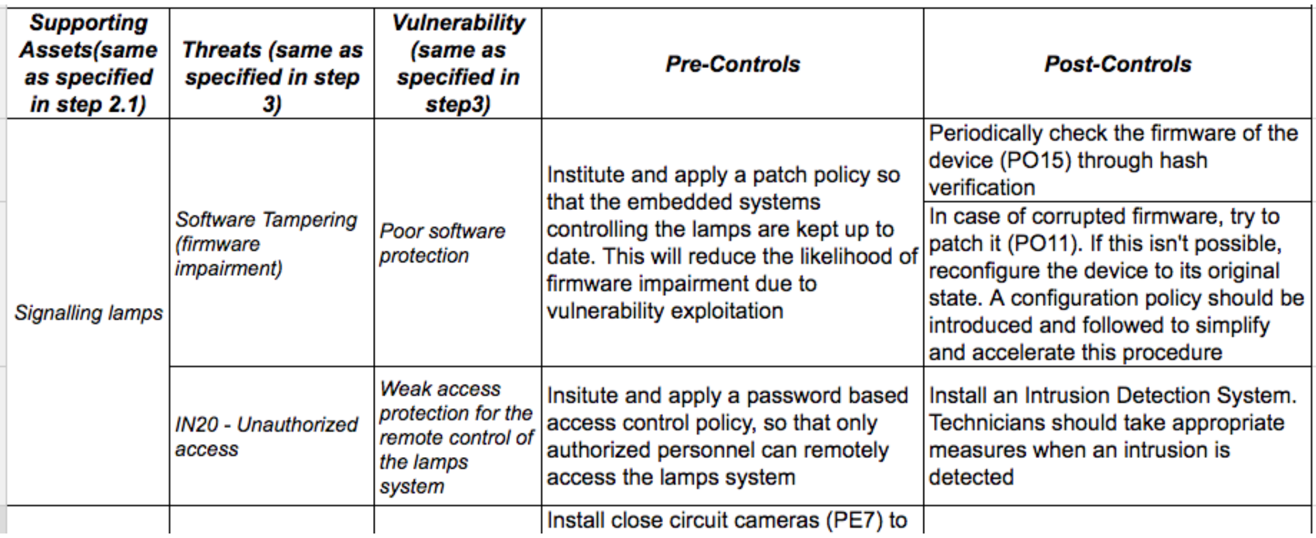
Visualization Systems	*(PH 8) Electro-Magnetic Interference*	*Electro magnetic interference with other devices*	PE14,PE15,PE25,PE26,PE29	PO8,PO10,PO12,PO17
	Destruction/ Vandalism	*Recorders easily accessible*	PE1,PE2,PE5,PE6,PE7,PE12,PE14, PE33,PE19,PE24,PE26,PE32	PO2,PO3, PO4,PO6,PO10,PO13,PO16
	Misconfiguration	*Recorders can show wrong data*	PE13,PE14,PE15,PE18,PE19,PE20, PE21,PE25	PO1,PO3,PO11,PO8,PO17
	Information share/disclosure	*People able to copy data recorded*	PE2,PE16,PE17,PE19,PE21,PE24,PE25,PE29,PE31	PO1,PO2,PO6,PO7,PO11,PO12,PO13,PO16,

Bad examples(2/2)



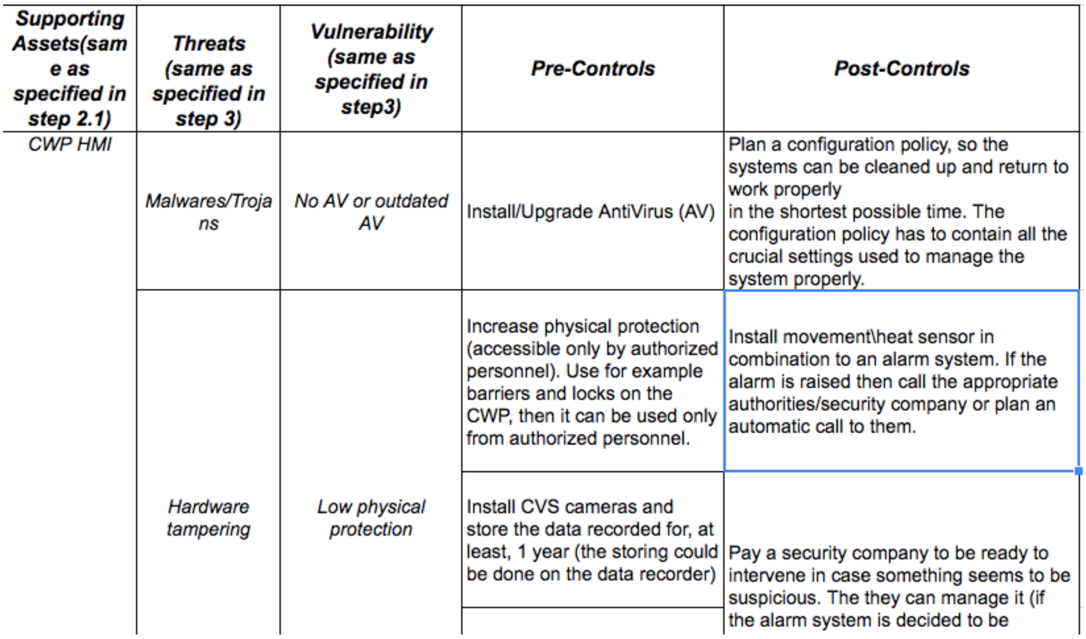
Supporting Assets(same as specified in step 2.1)	*Threats (same as specified in step 3)*	*Vulnerability (same as specified in step3)*	*Pre-Controls*	*Post-Controls*
SA1: Aircrafts & vehicles	*disclosure of sensitive information*	*no encryption*	usage of encryption	change control penestration testing
	data manipulation	*inadequate protection of data*	encoding data	anti-virus updates
	Threat C			
SA2: Personnel	*severe injury*	*lack of communication*	providing sufficient communication channels	improving the communication system
	Threat Z			

Good examples (1/2)



Supporting Assets(same as specified in step 2.1)	*Threats (same as specified in step 3)*	*Vulnerability (same as specified in step3)*	*Pre-Controls*	*Post-Controls*
Signalling lamps	*Software Tampering (firmware impairment)*	*Poor software protection*	Institute and apply a patch policy so that the embedded systems controlling the lamps are kept up to date. This will reduce the likelihood of firmware impairment due to vulnerability exploitation	Periodically check the firmware of the device (PO15) through hash verification In case of corrupted firmware, try to patch it (PO11). If this isn't possible, reconfigure the device to its original state. A configuration policy should be introduced and followed to simplify and accelerate this procedure
	IN20 - Unauthorized access	*Weak access protection for the remote control of the lamps system*	Insitute and apply a password based access control policy, so that only authorized personnel can remotely access the lamps system	Install an Intrusion Detection System. Technicians should take appropriate measures when an intrusion is detected
			Install close circuit cameras (PE7) to	

Good examples (2/2)



Supporting Assets(same as specified in step 2.1)	***Threats (same as specified in step 3)***	***Vulnerability (same as specified in step3)***	***Pre-Controls***	***Post-Controls***
CWP HMI	*Malwares/Trojans*	*No AV or outdated AV*	Install/Upgrade AntiVirus (AV)	Plan a configuration policy, so the systems can be cleaned up and return to work properly in the shortest possible time. The configuration policy has to contain all the crucial settings used to manage the system properly.
	Hardware tampering	*Low physical protection*	Increase physical protection (accessible only by authorized personnel). Use for example barriers and locks on the CWP, then it can be used only from authorized personnel.	Install movement\heat sensor in combination to an alarm system. If the alarm is raised then call the appropriate authorities/security company or plan an automatic call to them.
			Install CVS cameras and store the data recorded for, at least, 1 year (the storing could be done on the data recorder)	Pay a security company to be ready to intervene in case something seems to be suspicious. The they can manage it (if the alarm system is decided to be