Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET

Information Asset Risk	**Threat**	Information Asset	Archived Files
		Area of Concern	*Ransomware attack on personal devices*
		(1) Actor *Who would exploit the area of concern or threat?*	Malicious actor, most probably organized.
		(2) Means *How would the actor do it? What would they do?*	Abuse of smart device weakness or misconfigurations to access the home network and spread ransomware targeting other devices like personal computer and NAS.
		(3) Motive *What is the actor's reason for doing it?*	Financial gain
		(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☑ **Destruction** ☑ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Integrity, confidentiality and availability of files are breached.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** ☑ **Medium** □ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Payment of ransom or encryption of files contained in the infected device(s)	Reputation & Confidence	M	8
	Financial	H	15
Notable amount of time required to eradicate malware and restore device functionality.	Productivity	H	9
	Safety & Health	M	12
Potential loss of unique files and work.	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	9

Relative Risk Score **108**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

□ **Accept**	□ **Defer**	☑ **Mitigate**	☑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Files	Map relevant archived files and their archive locations to implement AV and security measures..
Files	Identify a trusted cloud backup service and synchronize the backups often. Be sure to have a local copy and a cloud copy for every relevant file. Local copies mitigate risk of availability breaches if the cloud is unreachable.
Network	Segment network to prevent spread of malware.
Offline backups	Use external hard drives to backup relevant files, keep them unplugged except for the short time strictly needed to access files. Unplugged HD can't be accessed by ransomware.

Allegro - Worksheet 10	**Information Asset Risk Worksheet**

Information Asset Risk	**Threat**	Information Asset	Archived Files
		Area of Concern	*Residual risk - Ransomware attack on personal devices*
		(1) Actor *Who would exploit the area of concern or threat?*	Malicious actor, most probably organized.
		(2) Means *How would the actor do it? What would they do?*	Abuse of smart device weakness or misconfigurations to access the home network and spread ransomware targeting other devices like personal computer and NAS.
		(3) Motive *What is the actor’s reason for doing it?*	Financial gain
		(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☑ **Destruction** ☑ **Modification** □ **Interruption**
		(5) Security Requirements *How would the information asset’s security requirements be breached?*	Integrity, confidentiality and availability of files are breached.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** □ **Medium** ☑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Relevant files backed up in cloud and offline drives can be restored. Loss of few recent assets not yet secured.	Reputation & Confidence	L	4
	Financial	L	5
Thanks to network segmentation, the malware can´ t spread to all devices, infection is contained to the IoT segment.	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
		Relative Risk Score	**25**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☑ **Accept**	□ **Defer**	□ **Mitigate**	□ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*