Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Internet connection		
		Area of Concern	*Abuse of weak WiFi authentication by unauthorized people*		
		(1) Actor *Who would exploit the area of concern or threat?*	External threat actor without advanced skills performing wifi attacks		
		(2) Means *How would the actor do it? What would they do?*	IoT devices have limited resources and rarely support the latest WiFi security standards. They are also an easy target for deauthentication attacks.		
		(3) Motive *What is the actor's reason for doing it?*	abuse of network bandwidth for personal purposes, potentially including illegal activities.		
		(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 the network impacted.		
		(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**
If the intruder gets unnoticed, he may perform illegal activities which could lead to the network owner facing legal consequences.	Reputation & Confidence	M	8
	Financial	L	5
Negative impact on network performances, affecting productivity and leading to increased costs.	Productivity	M	6
	Safety & Health	L	6
Confidentiality of data in the network is no longer ensured.	Fines & Legal Penalties	M	2
	User Defined Impact Area	L	2
		Relative Risk Score	**58**

(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?*
Network Access Credentials	Implement strong passwords and a regular password change policy.
Internet connection	Monitor internet traffic counters to detect abnormal traffic.
Networks	Configure router for network segmentation, divide Private network, IoT network and Guest network. Implement firewall rules to allow only necessary traffic.
Internet connection	Selectively allow internet connection only to trusted devices.

Allegro - Worksheet 10	Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Internet Connection	
		Area of Concern	*Execution of remote unauthorized activities*	
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organized Advanced Threat Actor	
		(2) Means *How would the actor do it? What would they do?*	Exploitation of firmware bugs and vulnerabilities in IoT devices leading to RCE and botnet.	
		(3) Motive *What is the actor's reason for doing it?*	Using IoT devices to proxy malicious traffic to anonymously attack other targets.	
		(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 seriously breached. availability impacted.	
		(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**
If the intruder gets unnoticed, he will perform illegal activities which could lead to the network owner facing legal consequences for the harm caused.	Reputation & Confidence	M	8
	Financial	L	5
Execution of remote activities could lead to increased power consumption, lower battery duration and additional traffic, impacting operative costs and performances.	Productivity	M	6
	Safety & Health	L	6
	Fines & Legal Penalties	H	3
	User Defined Impact Area	H	6
		Relative Risk Score	**34**

(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?*
Networks	Configure router for network segmentation, divide Private network, IoT network and Guest network. Implement firewall rules to allow only necessary traffic.
Network	Selectively allow internet connection only to trusted devices.
Network	Isolate IoT WiFi clients to prevent unnecessary cross-talking.

Allegro - Worksheet 10	Information Asset Risk Worksheet			
Information Asset Risk	**Threat**	Information Asset	Internet Connection	
		Area of Concern	*Execution of remote unauthorized activities - Residual risk*	
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organized Advanced Threat Actor	
		(2) Means *How would the actor do it? What would they do?*	Exploitation of firmware bugs and vulnerabilities in IoT devices leading to RCE and botnet.	
		(3) Motive *What is the actor's reason for doing it?*	Using IoT devices to proxy malicious traffic to anonymously attack other targets.	
		(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 seriously breached. availability impacted.	
		(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**
Execution of malware can lead to increased power consumption and lower battery duration, impacting operative costs and performances.	Reputation & Confidence	L	4
	Financial	L	5
	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	L	2
		Relative Risk Score	**21**

(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?*

Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Internet Connection		
		Area of Concern	*Lateral movement of threat actor in home network*		
		(1) Actor *Who would exploit the area of concern or threat?*	Individual or organized threat actor with technical skills.		
		(2) Means *How would the actor do it? What would they do?*	Exploited IoT device used as an entry point, allowing malicious actors to further exploit other devices, analyze network traffic and exfiltrate files.		
		(3) Motive *What is the actor's reason for doing it?*	Accessing sensitive data for financial gain (i.e. stealing credentials or blackmailing).		
		(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?*	Confidentiality and integrity of the network 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**
If the attack succeeds and sensitive data like logins are stolen, the threat actor can take control of the accounts, with potentially disastrous consequences for privacy and finance.	Reputation & Confidence	H	12
	Financial	H	15
If the attacker succeeds in exfiltrating personal files, he can use them for blackmailing or asking payment of a ransom to release them.	Productivity	H	9
	Safety & Health	M	12
The attacker may access work devices and files, harming not only the household members but also the organizations they work for.	Fines & Legal Penalties	M	2
	User Defined Impact Area	H	6
		Relative Risk Score	**56**

(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?*
Network	https
Network	strong passwords
Network	password change policy
Network	Network segmentation / Tri-band router
Devices	Software updates

Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Internet Connection		
		Area of Concern	*Reaching maximum number of clients / connections supported by router*		
		(1) Actor *Who would exploit the area of concern or threat?*	-		
		(2) Means *How would the actor do it? What would they do?*	Most consumer routers have a practical limit to the number of concurrent hosts or connections supported.		
		(3) Motive *What is the actor's reason for doing it?*	The limit can be easily reached when adding smart devices to home network		
		(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?*	Availability impacted		
		(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**
Instability and slowness of the network	Reputation & Confidence	L	4
	Financial	L	5
Possible crashes or reboots of router	Productivity	H	9
	Safety & Health	L	6
Inability of new devices to connect to the network	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
		Relative Risk Score	**62**

(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?*
Network	Configure a cascade router for network segmentation, divide Private network, IoT network and Guest network. Implement firewall rules to allow only necessary traffic. Use dedicated WiFi for IoT devices.

Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Threat	Information Asset	Internet Connection		
		Area of Concern	*Attacks to home gateway*		
		(1) Actor *Who would exploit the area of concern or threat?*	External threat, no specific skills needed		
		(2) Means *How would the actor do it? What would they do?*	After mapping open ports on the router using recon tools and fingerprinting exposed services, the home gateway is attacked using dictionary and brute force techniques or exploiting specific vulnerabilities.		
		(3) Motive *What is the actor's reason for doing it?*	Abusing gateway to exfiltrate data, distribute malware, lateral movement or C2C.		
		(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?*	Confidentiality and integrity of Home network 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**
In case of success, tampering of smart-home gateway and devices, including door locks, video cameras and other critical systems.	Reputation & Confidence	M	8
	Financial	L	5
Installation of malware on gateway, lateral movement, remote control and data exfiltration. Potential exposure of accounts and payment details stored on gateway, connected cloud services and iot devices. Attack of other devices in the network.	Productivity	H	9
	Safety & Health	M	10
In any case, abuse of computing resources impacts systems leading to poor performances, potential failures and unavailability.	Fines & Legal Penalties	M	2
	User Defined Impact Area	H	6
		Relative Risk Score	**120**

(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?*
Home Gateway	Prefer Cloudflare tunnels or webhook systems which allow external communication without opening ports on the router.
Home Gateway	Enable HTTPS if available
Network	Use WAF or firewall to limit maximum login attempts
Home Gateway	Keep software updated