DREAD Rating

DREAD Scale	
0	No Risk
3	Maximum Risk

WiFi Protected Setup (WPS)

Potential For: Brute Force Attack		
Category	**Score**	**Rationale**
Damage	3	Significant damage access point configuration.
Reproducibility	3	Well known vulnerability which can be reproduced with relative ease using widely available tools.
Exploitability	2	Easy to exploit at there are tools readily available tools to attack this vulnerability
Affected Users	3	All medical staff receiving training.
Discoverability	3	Discoverability always assumed at highest rating
	DREAD Score: 14	

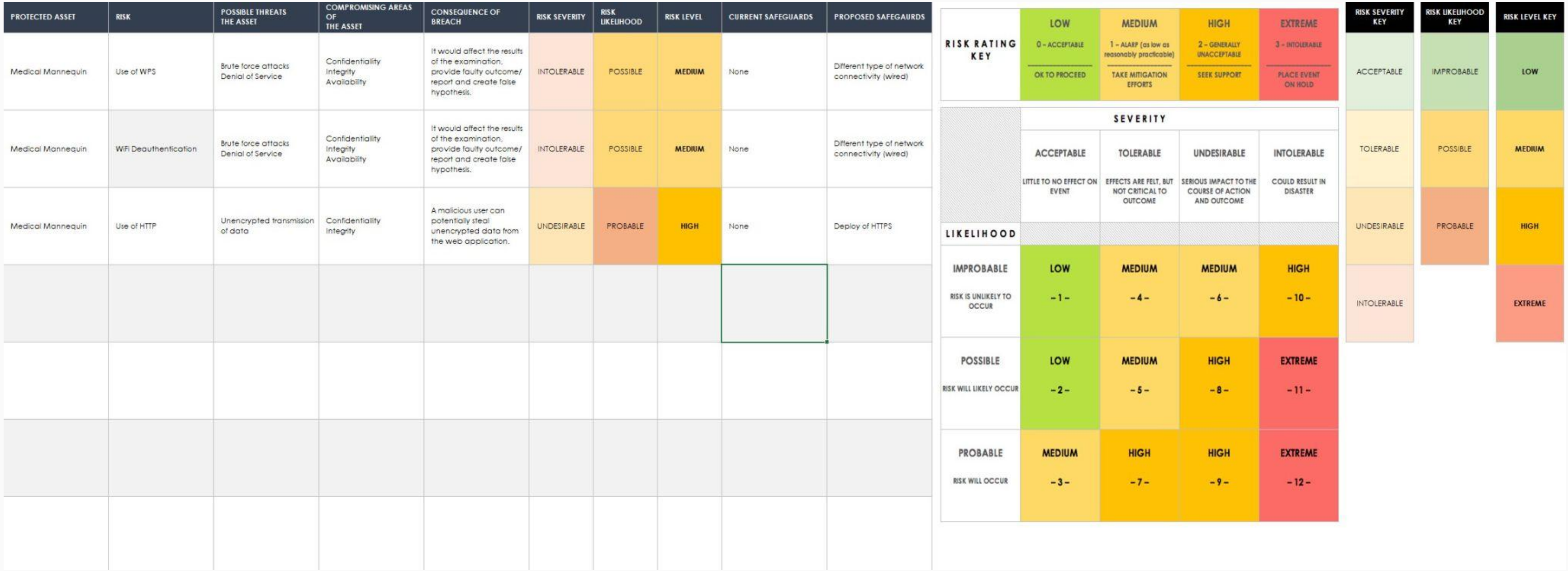
WiFi Deauthentication Attack

Potential For: Denial of Service

Category	**Score**	**Rationale**
Damage	3	Significant damage access point configuration.
Reproducibility	3	Well known vulnerability which can be reproduced with relative ease using widely available tools.
Exploitability	3	Easy to exploit at there are tools readily available tools to attack this vulnerability
Affected Users	3	All medical staff receiving training.
Discoverability	2	Discoverability always assumed at highest rating

DREAD Score: 14

Vulnerability Assessment Template



PROTECTED ASSET	RISK	POSSIBLE THREATS THE ASSET	COMPROMISING AREAS OF THE ASSET	CONSEQUENCE OF BREACH	RISK SEVERITY	RISK LIKELIHOOD	RISK LEVEL	CURRENT SAFEGUARDS	PROPOSED SAFEGAURDS
Medical Mannequin	Use of WPS	Brute force attacks Denial of Service	Confidentiality Integrity Availability	It would affect the results of the examination, provide faulty outcome/ report and create false hypothesis.	INTOLERABLE	POSSIBLE	**MEDIUM**	None	Different type of network connectivity (wired)
Medical Mannequin	WiFi Deauthentication	Brute force attacks Denial of Service	Confidentiality Integrity Availability	It would affect the results of the examination, provide faulty outcome/ report and create false hypothesis.	INTOLERABLE	POSSIBLE	**MEDIUM**	None	Different type of network connectivity (wired)
Medical Mannequin	Use of HTTP	Unencrypted transmission of data	Confidentiality Integrity	A malicious user can potentially steal unencrypted data from the web application.	UNDESIRABLE	PROBABLE	**HIGH**	None	Deploy of HTTPS

RISK RATING KEY	LOW	MEDIUM	HIGH	EXTREME
	0 - ACCEPTABLE	1 - ALARP (as low as reasonably practicable)	2 - GENERALLY UNACCEPTABLE	3 - INTOLERABLE
	OK TO PROCEED	TAKE MITIGATION EFFORTS	SEEK SUPPORT	PLACE EVENT ON HOLD

	SEVERITY			
	ACCEPTABLE LITTLE TO NO EFFECT ON EVENT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
LIKELIHOOD				
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW - 1 -	MEDIUM - 4 -	MEDIUM - 6 -	HIGH - 10 -
POSSIBLE RISK WILL LIKELY OCCUR	LOW - 2 -	MEDIUM - 5 -	HIGH - 8 -	EXTREME - 11 -
PROBABLE RISK WILL OCCUR	MEDIUM - 3 -	HIGH - 7 -	HIGH - 9 -	EXTREME - 12 -

RISK SEVERITY KEY	RISK LIKELIHOOD KEY	RISK LEVEL KEY
ACCEPTABLE	IMPROBABLE	**LOW**
TOLERABLE	POSSIBLE	**MEDIUM**
UNDESIRABLE	PROBABLE	**HIGH**
INTOLERABLE		**EXTREME**

Human Factor

Potential For: Denial of Service

Category	**Score**	**Rationale**
Damage	1	
Reproducibility	2	Well known vulnerability which can be reproduced with relative ease using widely available tools.
Exploitability	3	
Affected Users	3	
Discoverability	3	Discoverability always assumed at highest rating

DREAD Score: 12