

Threats Analysis Worksheet

Threat ID	Description	NEW		OLD		High Security		Enterprise		SOHO		Public		
		Priority	Severity	Priority	Severity	Priority	Severity	Priority	Severity	Priority	Severity	Priority	Severity	
T.DOS.NET.CONNECT	Opening all available network connections and keeping them open	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.DOS.NET.CRAFT	Sending crafted network packets to cause network interface failure	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.DOS.NET.FLOOD	Flooding packets to cause a sustained network interface failure	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.DOS.PRT.CRASH	Submitting PDL or print protocol data to cause print controller failure	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.DOS.PRT.DELETE	Submitting PDL or print protocol data to delete persistent resources	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.DOS.PRT.CHANNEL	Submitting PDL or print protocol data to backchannel message flood	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.DOS.PRT.PRIORITY	Intentionally continuously sending print jobs that de-prioritize other	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.DOS.FAX.HOOK	Inserting off-hook telephone in the loop	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.DOS.FAX.LOOP	Continuously sending/receiving grayscale fax pages at low speed	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.DOS.FAX.TRAIN	Forcing the fax modem to continuously train	2	1.8	1.9	1.3	2	1.8	1.9	2	1.8	1.9	3	1.8	2.3
T.DOS.FAX.VOLUME	Continuously sending excessive scanned document volume	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.DOS.PHY.ALTER	Mechanically or electrically altering or damaging the device or its cor	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.DOS.PHY.INTERFERE	Mechanically or electrically interfering with the device or its compone	2	2	2.0	1.4	2	2	2.0	2	2	2.0	3	2	2.4
T.RESOURCE.COPY	Using a rogue "copy" control device to bypass copy control	3	1.8	2.3	2.3	2	1.8	1.9	2	1.8	1.9	3	1.8	2.3
T.RESOURCE.PEER	Using a peer-to-peer connection to circumvent server security or acc	3	2	2.4	2.4	2	2	2.0	2	2	2.0	3	2	2.4
T.RESOURCE.SUPPLIES	Removing supplies or consumables	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.RESOURCE.EXHAUST	Submitting jobs to intentionally exhaust the device's consumables	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.UD.SNIFF.NET	Sniffing network traffic to gain access to documents	3	2.8	2.9	2.9	2	2.8	2.4	2	2.8	2.4	1	2.8	1.7
T.UD.SNIFF.EM	EM sniffing network traffic to gain access to documents	3	2.4	2.7	2.7	2	2.4	2.2	2	2.4	2.2	1	2.4	1.5
T.UD.SNIFF.PHONE	Tapping into a phone line to sniff fax traffic and gain access to faxed	3	2.6	2.8	2.8	2	2.6	2.3	2	2.6	2.3	1	2.6	1.6
T.UD.ACC.NORMAL	Electronically accessing another user's document using normal end u	3	2.2	2.6	2.6	2	2.2	2.1	2	2.2	2.1	1	2.2	1.5
T.UD.ACC.HACK	Electronically accessing another user's document in a non-standard i	3	2	2.4	2.4	2	2	2.0	2	2	2.0	1	2	1.4
T.UD.PHY.OUTPUT	Removing or examining documents from an output tray	3	2	2.4	2.4	2	2	2.0	2	2	2.0	3	2	2.4
T.UD.PHY.INPUT	Removing or examining documents from the document feeder	3	2	2.4	2.4	2	2	2.0	2	2	2.0	3	2	2.4
T.UD.PHY.CAMERA	Recording documents or user credentials using an internal or extern	3	2.4	2.7	2.7	2	2.4	2.2	2	2.4	2.2	1	2.4	1.5
T.UD.PHY.EM	Capturing EM radiation from device	3	2	2.4	2.4	2	2	2.0	2	2	2.0	1	2	1.4
T.UD.ANALYZE	Using electron microscope to read residual image on copier belt or d	3	1.6	2.2	2.2	2	1.6	1.8	2	1.6	1.8	1	1.6	1.3
T.UD.SALVAGE	Removing or swapping the device's hard disk	3	2.2	2.6	2.6	2	2.2	2.1	2	2.2	2.1	1	2.2	1.5
T.UD.IMP.FAX	Man-in-the-middle attack to alter inbound/outbound PSTN faxes	3	2	2.4	2.4	2	2	2.0	2	2	2.0	2	2	2.0

T.UD.IMP.PRINT	Man-in-the-middle attack to alter print jobs	3	2.2	2.6	2.6	2	2.2	2.1	2	2.2	2.1	2	2.2	2.1
T.UD.IMP.SCAN	Man-in-the-middle attack to alter scan or scan-to-fax data	3	2.2	2.6	2.6	2	2.2	2.1	2	2.2	2.1	2	2.2	2.1
T.TSF.CRED.NET	Sniffing network traffic to gain access to credentials	3	2.8	2.9	2.9	3	2.8	2.9	1	2.8	1.7	2	2.8	2.4
T.TSF.CRED.EM	EM sniffing network traffic to gain access to credentials	3	2	2.4	2.4	3	2	2.4	1	2	1.4	2	2	2.0
T.TSF.CRED.MGMT	Man-in-the-middle attack for management tools	3	2.2	2.6	2.6	3	2.2	2.6	1	2.2	1.5	2	2.2	2.1
T.TSF.CRED.DISK	Removing or swapping the device's hard disk or other persistent storage	3	2	2.4	2.4	3	2	2.4	1	2	1.4	2	2	2.0
T.TSF.CRED.GUESS	Obtaining credentials by guessing or observation	3	2.4	2.7	2.7	3	2.4	2.7	1	2.4	1.5	2	2.4	2.2
T.TSF.CONF.DEV	Changing the device settings or configuration	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.TSF.CONF.SEC	Changing the security settings or configuration	3	2.8	2.9	2.9	3	2.8	2.9	2	2.8	2.4	2	2.8	2.4
T.TSF.CONF.DATE	Changing device date/time for fax/SSL	3	2.2	2.6	2.6	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6
T.TSF.CONF.AB	Changing the address book to send copies of documents to other devices	3	2.6	2.8	2.8	2	2.6	2.3	2	2.6	2.3	3	2.6	2.8
T.TSF.SW.APPLET	Installing a rogue embedded software applet	3	2.2	2.6	2.6	3	2.2	2.6	2	2.2	2.1	3	2.2	2.6
T.TSF.SW.UPDATE	Installing a rogue firmware or software update	3	2	2.4	2.4	3	2	2.4	2	2	2.0	3	2	2.4
T.TSF.AUD.ACCESS	Accessing the device accounting/audit logs	3	2.4	2.7	2.7	3	2.4	2.7	2	2.4	2.2	2	2.4	2.2
T.TSF.AUD.ALTER	Altering the device accounting/audit logs	3	2.2	2.6	2.6	3	2.2	2.6	1	2.2	1.5	2	2.2	2.1
T.EA.PROXY	Propagating an attack to the local network through a network service	3	2	2.4	2.4	3	2	2.4	2	2	2.0	3	2	2.4
T.EA.DOS	Creating a denial-of-service attack on the local network through the	2	2.2	2.1	1.5	2	2.2	2.1	2	2.2	2.1	3	2.2	2.6

109.3 99.1

100.8

91.8

101.9

High Security
Enterprise
SOHO
Public

Must be considered
Should be considered