



Consolidated Assessment

Consolidated Management Plan



CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Scan Date: 2020/01/18

Prepared for: Your Customer /
Prospect

Prepared by: Your Company Name

2021/02/03

Table of Contents

01 | Network Management Plan







02 | Security Management Plan

Network Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILIT Y
97	<p>Upgrade or replace computers with operating systems that are no longer supported.</p> <ul style="list-style-type: none"> <input type="checkbox"/> ACCOUNTING / / Windows 7 Professional <input type="checkbox"/> CA-EXCHSVR / / Windows Server 2008 R2 Standard <input type="checkbox"/> IRGIS / / Windows Server 2008 R2 Standard <input type="checkbox"/> IRCAMA / / Windows Server 2008 R2 Standard <input type="checkbox"/> CA-VAL / fe80::510c:b8a1:f979:e69a%12,176.16.19.229 / Windows Server 2008 R2 Standard <input type="checkbox"/> MAPPINGSPAREHPP / / Windows 7 Professional <input type="checkbox"/> KYLE-HP308 / fe80::30c7:725d:9703:996e%11,176.16.19.61 / Windows 7 Professional <input type="checkbox"/> ibranaugh-hp400 / fe80::e8cd:a6c0:c33f:6686%11,176.16.19.15 / Windows 7 Professional <input type="checkbox"/> RKNIGHT-DESKPC / fe80::9d63:c248:6617:303c%15,176.16.19.39 / Windows 7 Professional <input type="checkbox"/> CA-AUTOMATE / fe80::e1:1cfe:77c7:f081%10,176.16.19.62 / Windows 7 Professional <input type="checkbox"/> CA-GIS / fe80::e87d:551d:a0e8:4d54%14,176.16.19.127 / Windows Server 2008 R2 Standard <input type="checkbox"/> CA-PRINTSVR / fe80::dde9:7211:4e7e:cc09%11,176.16.19.159 / Windows Server 2008 R2 Standard <input type="checkbox"/> FILESERVER1 / fe80::b5e1:f812:7adc:52c4%10,176.16.19.148 / Windows Server 2008 R2 Standard <input type="checkbox"/> FILESERVER2 / fe80::b957:c111:ed52:d7e1%10,176.16.19.12 	H	H

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILIT Y
	1 / Windows Server 2008 R2 Standard		
90	<p>Ensure anti-spyware definitions are up to date on specified computers.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Computer: CA-VAL IP Address: 176.16.19.229 Security Center: Windows Defender 		
90	<p>Ensure anti-virus definitions are up to date on specified computers.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Computer: CA-VAL IP Address: 176.16.19.229 Security Center: Windows Defender 		
75	<p>Address patching on computers missing 1-3 security patches.</p> <ul style="list-style-type: none"> <input type="checkbox"/> BRUCEHPZ230 / fe80::d9b8:475b:f9c3:2361%3,176.16.19.32 / Windows 10 Pro <input type="checkbox"/> FRNTCUSTSERVCUB / fe80::5ddc:510a:a3ec:478f%10,176.16.19.66 / Windows 10 Pro <input type="checkbox"/> KYLE-HP400 / fe80::80bb:fe3f:ae04:feb9%2,176.16.19.64 / Windows 10 Pro <input type="checkbox"/> CA-CSIMPSON / fe80::2802:1a6a:fd9:726f%7,176.16.19.35 / Windows 10 Pro <input type="checkbox"/> CA-DWHITE01 / fe80::7cd3:ac94:6a77:898e%11,176.16.19.30 / Windows 10 Pro <input type="checkbox"/> REMOTE-TL / fe80::8c22:bd00:80e5:e0ad%5,176.16.19.100 / Windows 10 Pro <input type="checkbox"/> SUSANHPUPGRD / fe80::20f9:9fef:618d:2dd2%6,176.16.19.87 / Windows 10 Pro <input type="checkbox"/> 1001westerfield-deskpc / fe80::e50e:653e:48fb:581a%10,176.16.19.36 / Windows 10 Pro <input type="checkbox"/> dwhiteacer / fe80::9d3d:4961:e31f:604f%3,176.16.19.98 / Windows 10 Pro <input type="checkbox"/> gilesmsi / fe80::91fb:c3ca:a191:371b%7,176.16.19.129 / Windows 10 Pro <input type="checkbox"/> sketteringprods khp / 		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

fe80::8c90:46f5:49f1:2d3a%5,176.16.19.101 /
Windows 10 Pro

Medium Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

68

Free or add additional disk space for the specified drives.

H

L

- REMOTE-TL - E : 0.06 GB free
- KYLE-HP400 - E : 0.09 GB free
- sketteringprodskhp - E : 0.06 GB free
- ibranaugh-hp400 - E : 0.06 GB free

Low Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

30

Investigate all accounts with passwords set to never expire and configure them to expire regularly.

L

L

- IRCPA.ORG\Administrator / Administrator
- IRCPA.ORG\ITSupport / Information System.
- IRCPA.ORG\RKnight / Riley Knight
- IRCPA.ORG\SQLServerGIS / SQLServerGIS
- IRCPA.ORG\SQLSVRRun / SQLSVR Run
- IRCPA.ORG\TA01 / True Automation







20

Upgrade computers that have operating systems in Extended Support before end of life.

L

L

- CA-IIS / / Windows Server 2012 R2 Standard
- CA-GISTEST / fe80::2169:f451:ed24:29af%13,176.16.19.68 /

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	Windows Server 2012 R2 Standard		
15	<p>Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, logged into by authorized users, or powered on.</p> <ul style="list-style-type: none"> <input type="checkbox"/> 4001WAYNEG-CA / 176.16.19.24 / Windows 10 Pro <input type="checkbox"/> 1001westerfield-deskpc / fe80::e50e:653e:48fb:581a%10,176.16.19.36 / Windows 10 Pro 		
13	<p>Disable or remove user accounts for users that have not logged on to active directory in 30 days.</p> <ul style="list-style-type: none"> <input type="checkbox"/> WFRCMBR\$ / WFRCMBR\$ <input type="checkbox"/> Administrator / Administrator <input type="checkbox"/> ASmith / Axel Smith <input type="checkbox"/> BGodwin / Bruce Godwin <input type="checkbox"/> CSimpson / Charlie Simpson <input type="checkbox"/> DWhite / Daniel White <input type="checkbox"/> GHarris / Giles Harris <input type="checkbox"/> GIS / GIS <input type="checkbox"/> IBranaugh / Ira Branaugh <input type="checkbox"/> ITSupport / Information System. <input type="checkbox"/> JShearing / James Shearing <input type="checkbox"/> KSulu / Kyle Sulu <input type="checkbox"/> MTalman / Millie Talman <input type="checkbox"/> RKnight / Riley Knight <input type="checkbox"/> Sales / Sales <input type="checkbox"/> SKettering / Skyla Kettering <input type="checkbox"/> SQLSVRRun / SQLSVR Run <input type="checkbox"/> SQLServerGIS / SQLServerGIS <input type="checkbox"/> SBorne / Susan Borne <input type="checkbox"/> travis / Travis King <input type="checkbox"/> TA01 / True Automation <input type="checkbox"/> VWesterfield / Val Westerfield <input type="checkbox"/> WGreen / Wayne Green 		
10	<p>There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they often lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be</p>		

RISK
SCORE

RECOMMENDATION

SEVERITY

PROBABILIT
Y

reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security. See Listening Ports sheets in Excel Export for details.

- BRN001BA9F02883.IRCPA.ORG
(176.16.19.13)
- 176.16.19.17
- 176.16.19.14
- 176.16.19.38
- NPIE0AD8C.IRCPA.ORG
(176.16.19.48)
- BRN30055CA859DF.IRCPA.ORG
(176.16.19.56)
- 176.16.19.53
- NPI811FE6.IRCPA.ORG
(176.16.19.58)
- NPI3DCDB7.IRCPA.ORG
(176.16.19.59)
- 176.16.19.95
- 176.16.19.99
- HPSCANNER (176.16.19.131)
- NPIB54250 (176.16.19.140)
- BRN30055C5D33E4 (176.16.19.178)
- BRN30055C7A1552 (176.16.19.214)
- BRN30055C664B57 (176.16.19.225)
- BRN30055CA7DBCD (176.16.19.235)
- 176.16.19.160
- BRN30055C7A390A (176.16.19.245)
- NPIB913C8 (176.16.19.242)
- NPIF0D692 (176.16.19.224)
- REALESTATE.IRCPA.ORG
(176.16.19.241)
- 176.16.19.254
- S1016372.IRCPA.ORG
(176.16.19.250)
- HPT1300.IRCPA.ORG (176.16.19.130)
- 176.16.19.158
- 4001WAYNEG-CA.IRCPA.ORG
(176.16.19.24)

Security Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILIT Y
77	Enable account lockout for all users.	H	H
75	<p>Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Name: Missing `httpOnly` Cookie Attribute / CVSS: 5 / IP: 66.11.8.80 <input type="checkbox"/> Name: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection / CVSS: 4.3 / IP: 66.11.8.80 <input type="checkbox"/> Name: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability / CVSS: 4 / IP: 66.11.8.80 <input type="checkbox"/> Name: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS / CVSS: 5 / IP: 66.11.8.80 <input type="checkbox"/> Name: SSL/TLS: Report Weak Cipher Suites / CVSS: 4.3 / IP: 66.11.8.80 <input type="checkbox"/> Name: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) / CVSS: 4.3 / IP: 66.11.8.80 	H	H
75	Enable enforcement of password length to more than 8 characters.	H	M
75	<p>Enable password complexity to assure that network user account passwords are secure.</p> <ul style="list-style-type: none"> <input type="checkbox"/> GENAVE-PC <input type="checkbox"/> ibranaugh-hp400 <input type="checkbox"/> INSP-TEST2 <input type="checkbox"/> milliehpz240 	H	H

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
72	Increase password history to remember at least six passwords.	H	H
72	Enable automatic screen lock on the specified computers. <input type="checkbox"/> GENAVE-PC <input type="checkbox"/> INSP-TEST2	M	M

Medium Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
70	Modify the maximum password age to be 90 days or less.	H	L
68	Eliminate inconsistencies and exceptions to the password policy.	H	H
68	Reduce screen lockout to 15 minutes or less on the specified computers. <input type="checkbox"/> 1001westerfield-deskpc <input type="checkbox"/> dwhiteacer <input type="checkbox"/> gilesmsi <input type="checkbox"/> ibranaugh-hp400 <input type="checkbox"/> milliehpz240 <input type="checkbox"/> sketteringprodskh	M	M

Low Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
50	Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess. Only the first 5 per domain are listed here. <input type="checkbox"/> dstaar@ircpa.org password: jord*****	H	L

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<ul style="list-style-type: none"><input type="checkbox"/> lchavis@ircpa.org password: chie*****<input type="checkbox"/> mstrickland@ircpa.org password: mont*****<input type="checkbox"/> nneill@ircpa.org password: vero*****		
50	Ensure company's WiFi is secure and discourage the use of any open WiFi connections.	L	L