YourIT!
Your Logo Goes Here

PCI Assessment

PCI Management Plan

Prepared for:
Prospect or Customer
Prepared by:
Your Company Name

3/29/2016

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 global 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	Probability
100	**PCI DSS Requirement 3.2 - Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.** Identify and remove the source resulting in storage of Primary Account Numbers (PAN) in the file system. ☐ Corp.MyCorp.com\PITMARC-PC: C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SmbShare\en-US\SmbOpenFile.cdxml-help.xml ☐ Corp.MyCorp.com\PITMARC-PC: E:\ECOMM Documents Folder\Rapid Fire Tools\SAM and NAM Sample Reports\Network\Full Detail Report.docx	H	H
95	**PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).** Enable antispyware on all computers commonly affected by malicious software. ☐ HYPER04 / 192.168.1.104 / Windows Server 2012 R2 Datacenter ☐ CORY-WIN7 / 192.168.6.44 / Windows 7 Enterprise ☐ HYPER01 / 192.168.1.111 / Windows Server 2012 R2 Standard ☐ UTIL-1 / 192.168.1.15 / Windows Server 2012 R2 Standard ☐ OPSTFS / 192.168.1.16 / Windows Server 2012 Standard ☐ HYPER02 / 192.168.1.121 / Windows Server 2012 R2 Standard ☐ TSUMMER-WIN764 / 192.168.7.18 / Windows 8.1 Enterprise ☐ RD-GATE / 192.168.1.21 / Windows Server 2012 R2 Datacenter ☐ TS01 / 192.168.6.80 / Windows Server 2012 R2 Standard ☐ TSUMMER-PC / 192.168.6.40 / Windows 8.1 Pro ☐ FS-2012 / 192.168.1.41 / Windows Server 2012 R2 Standard ☐ HYPER00 / 192.168.1.100 / Windows Server 2012 R2 Datacenter ☐ VPNGW / 192.168.1.5 / Windows Server 2012 R2 Standard ☐ OPSTFSBUILD / 192.168.6.67 / Windows Server 2012 R2 Standard	H	H
95	**PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly**	H	H

Risk Score	Recommendation	Severity	Probability
	personal computers and servers). Enable antivirus on all computers commonly affected by malicious software. ☐ TSUMMER-WIN7TEST / 192.168.6.53 / Windows 7 Professional ☐ HYPER04 / 192.168.1.104 / Windows Server 2012 R2 Datacenter ☐ CORY-WIN7 / 192.168.6.44 / Windows 7 Enterprise ☐ HYPER01 / 192.168.1.111 / Windows Server 2012 R2 Standard ☐ UTIL-1 / 192.168.1.15 / Windows Server 2012 R2 Standard ☐ OPSTFS / 192.168.1.16 / Windows Server 2012 Standard ☐ HYPER02 / 192.168.1.121 / Windows Server 2012 R2 Standard ☐ TSUMMER-WIN764 / 192.168.7.18 / Windows 8.1 Enterprise ☐ RD-GATE / 192.168.1.21 / Windows Server 2012 R2 Datacenter ☐ TS01 / 192.168.6.80 / Windows Server 2012 R2 Standard ☐ TSUMMER-PC / 192.168.6.40 / Windows 8.1 Pro ☐ FS-2012 / 192.168.1.41 / Windows Server 2012 R2 Standard ☐ HYPER00 / 192.168.1.100 / Windows Server 2012 R2 Datacenter ☐ CONFERENCEROOM / 192.168.6.33 / Windows 7 Professional ☐ VPNGW / 192.168.1.5 / Windows Server 2012 R2 Standard ☐ OPSTFSBUILD / 192.168.6.67 / Windows Server 2012 R2 Standard		
94	**PCI DSS Requirement 1.1.6 - Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.** Close or unpublish external facing ports using inherently insecure protocols or provide additional security features and documentation. ☐ 42.26.150.2 : 80/tcp (http)	H	H
92	**PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).** Update antispyware definitions to ensure protection against the latest threats. ☐ WS-1 / 192.168.6.97 / Windows 8 Enterprise	H	H
92	**PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).** Update antivirus definitions to ensure protection against the latest threats. ☐ WS-1 / 192.168.6.97 / Windows 8 Enterprise ☐ CONFERENCEROOM / 192.168.6.33 / Windows 7 Professional	H	H
92	**PCI DSS Requirement 2.3.b - Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.**	H	H

Risk Score	Recommendation	Severity	Probability
	Block or disable access to Telnet and other insecure remote-login commands for non-console access. ☐ HTTP (80/TCP) on HHOLT-DT (192.168.7.45) / 80 ☐ HTTP (80/TCP) on OPS-1 (192.168.7.65) / 80 ☐ HTTP (8080/TCP) on OPS-1 (192.168.7.65) / 8080 ☐ HTTP (80/TCP) on WS-2 (192.168.7.89) / 80		
89	**PCI DSS Requirement 10.2.2 - All actions taken by any individual with root or administrative privileges.** Enable auditing of all actions taken by any individual with root or administrative privileges.	H	M
87	**PCI DSS Requirement 1.3.5 - Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.** Block web traffic to all sites not required by the CDE. ☐ http://espn.go.com ☐ http://gmail.google.com ☐ http://isohunt.to ☐ http://mail.yahoo.com ☐ http://thepiratebay.se ☐ http://www.cnet.com ☐ http://www.facebook.com ☐ http://www.myspace.com ☐ http://www.playboy.com ☐ http://www.tucows.com ☐ http://www.youporn.com ☐ http://www.youtube.com ☐ https://plus.google.com ☐	H	H
83	**PCI DSS Requirement 8.2.3 - Passwords/phrases must meet the following: * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.** Enforce password complexity of at least 7 characters and contain both numeric and alphabetic characters.	M	H
81	**PCI DSS Requirement 8.2.5 - Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.** Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	M	H
77	**PCI DSS Requirement 8.1.6 - Limit repeated access attempts by locking out the user ID after not more than six attempts.** Ensure password lockout is enforced after more than six attempts.	M	H
77	**PCI DSS Requirement 2.2.3 - Implement additional security features**	M	H

Risk Score	Recommendation	Severity	Probability
	for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. ☐ HHOLT-DT.CORP.PERFORMANCEIT.COM / 80 ☐ OPS-1.CORP.PERFORMANCEIT.COM / 80 ☐ OPS-1.CORP.PERFORMANCEIT.COM / 8080 ☐ WS-2.CORP.PERFORMANCEIT.COM / 80		
75	**PCI DSS Requirement 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.** Address patching on computers with missing security patches. ☐ DC-3 / 192.168.1.23, 192.168.1.4, 192.168.1.3 ☐ JACK-WIN8 / 192.168.7.44	M	H
74	**PCI DSS Requirement 8.1.7 - Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	M	H
72	**PCI DSS Requirement 8.1.3 - Immediately revoke access for any terminated users.** Disable or remove accounts for former employees and vendors. ☐ mwest / Mary West ☐ cweston / Candy Weston	M	M

Medium Risk

Risk Score	Recommendation	Severity	Probability
70	**PCI DSS Requirement 8.1.1 - Assign all users a unique ID before allowing them to access system components or cardholder data.** Investigate and either disable or note compensating controls to ensure these potential generic accounts are not used inappropriately. Service accounts are excluded. ☐ Corp.MyCorp.com\admin ☐ Corp.MyCorp.com\Administrator ☐ Corp.MyCorp.com\sales ☐ Corp.MyCorp.com\support ☐ Corp.MyCorp.com\DDRTest ☐ Corp.MyCorp.com\SUPPORT$	M	M

Risk Score	Recommendation	Severity	Probability
	☐ Corp.MyCorp.com\supportguy ☐ Corp.MyCorp.com\nonadminuser ☐ Corp.MyCorp.com\marty-test ☐ Corp.MyCorp.com\Tester		
69	**PCI DSS Requirement 10.2.5 - Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.** Enable auditing of changes to account identification and authentication mechanisms.	M	M
67	**PCI DSS Requirement 8.1.5 - Manage IDs used by vendors to access, support, or maintain system components via remote access** Disable vendor accounts when not in use. ☐ dperry / David Perry	M	M
62	**PCI DSS Requirement 8.1.3 - Immediately revoke access for any terminated users.** Investigate and determine if the users are former employees or vendors. ☐ admin / admin admin ☐ adminonly / admin only ☐ jcosmore / Jsff Cosmore ☐ tmorret / t morret ☐ mwest / Mary West ☐ mwilder / Mike Wilder ☐ hr / MyCorp HR ☐ partners / MyCorp Managed Services Partners ☐ info / MyCorp PR ☐ sraki / Steve Rakie. ☐ cweston / Candy Weston ☐ slouder / Sarah Louder	M	L
62	**PCI DSS Requirement 8.1.5 - Manage IDs used by vendors to access, support, or maintain system components via remote access** Disable or remove accounts for former employees and vendors.	M	L
60	**PCI DSS Requirement 1.1.4.b - Verify that the current network diagram is consistent with the firewall configuration standards.** Updated the network diagram to be consistent with the requirement to deploy a firewall at each Internet connection or note in the CCW any exceptions.	M	M

Low Risk

Risk Score	Recommendation	Severity	Probability
50	**PCI DSS Requirement 6.5 - Address common coding vulnerabilities in software-development processes** Establish a program to train developers on secure coding guidelines to protect applications.	M	M