How SkyView Products Assist with PCI Compliance

The Payment Card Industry has a published set of Data Security Standards to which organization's accepting and storing credit card information must adhere. Since these Data Security Standards apply to all systems, one must do some interpretation to determine how the requirements apply to i5/OS and OS/400. While some specifications are clearly spelled out (such as the password requirements) others are defined by their intent.

The Data Security Standard's intent is that the integrity of your data can be assured, access to your data is restricted, and your systems' security scheme is configured to support this intent. To accomplish this, you need a comprehensive review of your security.

Solution: **SkyView Partners' Risk Assessor for i5/OS & OS/400**
(See: http://skyviewpartners.com/pdf/RiskAssessorFactSheet.pdf)

Risk Assessor compares your system's security configuration against security best practices for over 100 risk points, including system values, user profile settings, object level authorities, TCP/IP configuration, file shares and much more. Risk Assessor provides an explanation of the issue to allow you to determine whether the issue requires remediation. If remediation is required, Risk Assessor provides suggestions on how to start the remediation process. In essence, Risk Assessor gives you a "third-party expert" review of your security.

Risk Assessor specifically addresses the requirement for "an annual process that identifies threats and vulnerabilities, resulting in a risk assessment."

Beyond Risk Assessor's unique ability to help you ensure that your systems' configuration supports the intent of the Data Security Standard on i5/OS, there are also numerous specific Data Security Standards requirements. In each of the following you must define your own policy and prove your compliance.

Solution: **SkyView Partners' Policy Minder for i5/OS & OS/400**
(See: http://www.skyviewpartners.com/pdf/Policy_Minder_Data_Sheet.pdf)

Policy Minder makes monitoring and maintaining the implementation details of your security policy easy and takes the guesswork out of your security compliance status. Here are some more specific examples:

Data Security Standards require detection of default passwords.

Solution: Policy Minder can check EVERY user profile configuration to ensure no profiles have default passwords. (Note: you may have third-party vendor software that ships a profile with a default password and cannot be changed. Using Policy Minder, you can define the no default password policy and then omit any profiles that are an exception to this rule. Your policy, including the exceptions, is now documented for the auditors.)

Data Security Standards require "strong access controls."

Solution: In i5/OS terms this means that database files containing cardholder data be set to public authority *EXCLUDE. Policy Minder can help you change this setting as well as perform regular compliance checks to ensure the files remain secured appropriately. If users are specifically allowed access, this can also be included in the check.

Data Security Standards require that inactive profiles be removed from the system at least every 90 days.

Solution: Policy Minder can simplify the discovery and automate the removal of inactive profiles. Beginning in Version 1.3, you can use Policy Minder to find and take action on inactive profiles. These capabilities include the ability to set the status to *DISABLED on profiles that are inactive for a specified number of days, as well as automatically delete profiles after a specified number of days of inactivity.

Data Security Standards require proper user profile configuration

Solution: Policy Minder can be used to ensure profiles are created (or changed) with the correct special authorities, group assignments, initial programs, auditing settings, and more. For example, Policy Minder can be used to identify new profiles that have been created, changed or restored that now have *ALLOBJ (security officer) authority.

Data Security Standards require all users' passwords be changed every 90 days

Solution: Policy Minder can be used to check your system values to ensure that i5/OS passwords are changed every 90 days. In addition, it can ensure that the systems' password composition rules meet the Standards' password requirements.

Data Security Standards require that policies be documented.

Solution: Policy Minder can be used to generate a PDF file showing your policies as they have been defined within Policy Minder. You could use this report for your documentation for the i5/OS implementation of your overall security policy to show auditors as to how your security is configured, the user profile attributes you are monitoring as well as the specific objects you are monitoring for security compliance. Also, an additional description can be added to the policy to explain the purpose of the policy or refer to a corporate security policy, document risk acceptance statements, etc.

Data Security Standards require that security configurations be tested regularly.

Solution: Policy Minder generates compliance check reports, providing proof to auditors that you are regularly monitoring your i5/OS security configuration. If the item being checked is in compliance (meaning that it meets the requirements of your policy), a one-page summary report is generated stating that the item(s) are in compliance with the policy requirements. If the item is out of compliance, the report contains a detailed description of the discrepancy.

These are just some of the ways you can use SkyView Partners' products to assist with PCI compliance. For more information on our products and services, I encourage you to visit our website at www.skyviewpartners.com.

About the author:

Carol Woodbury *is President and co-founder of SkyView Partners, Inc. and is the designer and architect of the SkyView Partners' products. Carol has over 17 years in the security industry, 10 of those working the AS/400 Security Architect and Chief Engineering Manager of Security Technology of Security Technology for IBM's Enterprise Server Group. Carol's second book, Experts' Guide to OS/400 and i5/OS Security, is available at www.amazon.com .*