



PCI COMPLIANCE: AN OVERVIEW

by Alain Sadeghi

Is your business PCI compliant? Do you even know what PCI compliance is? Does your business accept credit cards, especially Visa and MasterCard? If so, then you need to know about PCI compliance and how it can affect your business.

Before we get into an explanation of PCI compliance and its requirements, we have to go into a little history.

Beginning in June of 2001, Visa introduced their Cardholder Information Security Program (CISP) to help protect cardholder data. This program outlined fundamental security requirements for all Visa merchants and service providers.

MasterCard created their program, known as the MasterCard Site Data Protection Program (SDP). Their program was designed to help issuers, acquirers, retailers, and service providers protect themselves and the overall payment system against the threat of compromises.

In December of 2004, Visa and MasterCard joined forces and officially announced the combination of Visa's CISP and MasterCard's SDP programs. Together, they recognized the need for a common set of security requirements and a single validation process for merchants and service providers. The result of this collaboration is the Payment Card Industry (PCI) Data Security Standard. Since 2004, American Express and Discover Card have also approved this Standard within their own programs.

There are 12 requirements in the PCI Data Security Standard:

- **Build and Maintain a Secure Network**
 1. Install and maintain a firewall configuration to protect data.
 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
- **Protect Cardholder Data**
 3. Protect stored data.
 4. Encrypt transmissions of cardholder data and sensitive information across public networks.
- **Maintain a Vulnerability Management Program**
 5. Use and regularly update anti-virus software.
 6. Develop and maintain secure systems and applications.
 7. Restrict access to data by business need-to-know.

8. Assign a unique ID to each person with computer access.
 9. Restrict physical access to cardholder data.
- **Regularly Monitor and Test Networks**
 10. Track and monitor all access to network resources and cardholder data.
 11. Regularly test security systems and processes.
 - **Maintain an Information Security Policy**
 12. Maintain a policy that addresses information security.

Now as we all know it does not do any good to have rules (or standards) if they are not enforced. Therefore, one of the main parts of the PCI Data Security Standard success is merchant and service provider compliance. When the Standard's requirements are enforced, they can serve as a defense against data exposure and compromise. Part of this compliance is a required on-site PCI validation assessment conducted by an approved Qualified Data Security Company (QDSC).

You may be asking yourself—what happens to companies who fail to meet the PCI Data Security Standard. The companies who do not comply can be fined, have restrictions imposed on them, and/or expelled from the Payment Card System. In short, if you chose not to address PCI compliance for your business you may very well find yourself unable to accept Visa, and possibly American Express and/or Discover Card.

Now ask yourself how that would affect your bottom line?

For more information on this article, contact info@etechsecurity.com.

About the Author

Alain Sadeghi is the CTO of eTechSecurity and the founding member of the Information Systems Security Association (ISSA) Tri-Cities Chapter. He has studied both at Sorbonne and Berkeley Universities and he holds a bachelor's degree in International Economics and a Master's degree in Computer Science as well as numerous other industry and vendor certifications including a CISSP, CISA, and CISM. Alain has spent approximately 20 years in IT management both nationally and internationally. He has worked in partnership with IBM, EDS, Cisco, HP, Microsoft and other Fortune 500 companies on a variety of IT projects.