PCI and Remote Support: How Compliant are the Keys to the Kingdom?

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Bomgar Corporation
May 2011
Table of Contents

Executive Summary ............................................................................................................................................1

The PCI Challenge...........................................................................................................................................1

  PCI and Remote Support: Protecting the Keys to the Kingdom.................................................................1

  Remote Support and PCI Scope .................................................................................................................2

  Assuring the Integrity of Control..............................................................................................................2

A Case Study ...................................................................................................................................................3

EMA Perspective............................................................................................................................................4

About Bomgar ..............................................................................................................................................4
Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) is one of the most referenced regulatory initiatives affecting IT organizations. It is also one of the most prescriptive, with specific requirements in multiple domains for businesses that handle personally identifiable information linked to payment accounts. Among these are requirements for securing access to subject systems for the purposes of IT support and other administrative functions.

This is one of the most sensitive aspects of IT access in any organization—and the PCI DSS treats it accordingly. In this paper, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts examine the requirements of the PCI Data Security standard for remote and administrative support access, and the emphasis it places on network security, strong authentication, and verifiable integrity. Related issues such as requirements for outsourced environments are also considered in evaluating the scope of compliance in this area. The paper concludes with a case study that highlights one organization’s choice of a self-hosted collaborative remote support solution that helps a $4 billion leader in hospitality and retail technology meet the requirements of PCI to deliver security, visibility, and reliability for both this company and its supported customers.

The PCI Challenge

Payment account information has tangible value that can be directly exploited through credit card fraud and other means. The PCI DSS is the payment card industry’s recognition that those who handle Personally Identifiable Information (PII) have a responsibility to keep it confidential and safe. High-profile breach events have accentuated this responsibility, and have contributed to the development of a comprehensive set of PCI DSS requirements for businesses that handle payment card data. These requirements continue to evolve along with the progress of technology, as emerging trends such as virtualization and the proliferation of Web technologies continue to define the business data center.

Much attention has been given to PCI requirements that focus on well-known IT security tactics such as network defense, vulnerability assessment and data encryption. This does not mean, however, that other requirements are any less significant.

PCI and Remote Support: Protecting the Keys to the Kingdom

For example, the PCI DSS includes requirements for strong controls on access to cardholder data management systems—but organizations need to fully consider what this means, particularly when it comes to technologies that enable support teams to access and fix IT resources. This type of access for IT support purposes often means the ability to directly view and control systems that handle sensitive cardholder data. It may also mean the ability to manipulate a wide range of controls required for PCI compliance—including the ability to compromise these controls. Even when it does not mean such direct control, support access may be the door through which more sensitive access can be obtained.
This places a much higher premium on measures for assuring the compliance of support access than many organizations may have considered. Organizations should therefore consider some important factors in their choice of techniques for enabling remote access for IT administration and support.

Remote Support and PCI Scope
Before organizations even begin to assess the strength and integrity of controls over administrative and support access, they may first want to consider the scope of their efforts. Organizations subject to PCI DSS compliance should be aware that they are responsible for access to the cardholder data environment within the scope of their compliance obligations. The PCI DSS is clear about measures for securing direct access to administrative control over the cardholder data environment on the part of the PCI-compliant organization itself—but where requirements may be less clear is when administrative access is not so direct.

For example, Requirement 12.8 addresses responsibilities when cardholder data is shared with service providers, while Appendix A speaks to requirements for shared hosting providers. At the same time, however, the preamble to Appendix A of PCI DSS version 2 states that “all service providers with access to cardholder data” must adhere to the PCI DSS. If, for example, organizations use a third-party service to enable remote support access to the cardholder data environment, they will want to verify with their Qualified Security Assessors (QSAs) the measures that are necessary to assure that the service is either out of scope of, or in compliance with the PCI DSS.

Assuring the Integrity of Control
Where the PCI DSS is clear is in regards to the use of measures such as two-factor authentication for remote access on the part of employees, administrators and third parties (Requirement 8.3). The Standard requires a unique ID for each user accessing system components or cardholder data (Requirement 8.1), as well as “at least one of the following methods to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smartcard; [and] something you are, such as a biometric” (Requirement 8.2). Requirement 8 covers a number of other aspects of user account and password management, such as prohibitions against the use of group, shared or generic accounts and passwords, and specific requirements for user account and password lifecycle management. Requirement 9 speaks to the need for controls over physical access to cardholder data.

The PCI DSS also has specific requirements for securing remote administrative access to the cardholder data environment, such as encryption of all non-console administrative access. Requirement 2.3 specifically mandates the use of technologies such as SSH (Secure Shell), VPN (Virtual Private Network), or SSL/TLS (Secure Sockets Layer/Transport Layer Security) for this purpose.

The reason this is important is reflected in Requirement 1.2, which mandates the restriction of network connections “between untrusted networks and any system components in the cardholder data environment.” Requirement 1.2 describes an “untrusted network” as “any network that is external to

Is Support Putting you at Risk?
IT and security executives should ask:

- Is your support team using strong authentication and unique IDs for remote access?
- Are you using a hosted remote access solution, and if so, does your service provider adhere to PCI DSS?
- Can you ensure end-to-end integrity and control of the systems being used to remotely access your sensitive data?

1 Emphasis EMA's
the networks belonging to the entity under review, and/or which is out of the entity’s ability to control or manage.” When passing through such networks, the communication of sensitive administrative credentials and access to high-privilege control must be protected.

This suggests how the integrity of remote administrative or support access requires end-to-end protection and control. The confidentiality and safety of sensitive administrative credentials and high-privilege access must be assured from the interface with administrative or support personnel, all the way to the target system. Organizations that cannot ensure such end-to-end integrity and control must consider what it would take to provide compensating controls, not only in terms of adding complexity to their remote support techniques, but potentially adding significant cost—if such controls can be provided at all.

### A Case Study

One company that weighed its options for remote access technology for administrative access and IT support made its choice in large part because of these requirements of the PCI DSS. MICROS Systems Inc., a Columbia, Maryland-based company of $4 billion in market capitalization and nearly 5,000 employees, develops, deploys and supports enterprise point-of-sale and property management systems for the hospitality and retail markets. Clearly, PCI is front-and-center when it comes to MICROS’s selection for remote support of its products among its customer base.

MICROS’s options included the hosted remote support technologies of third-party service providers, as well as technologies it could own and deploy completely under its own control. After experience with a third-party hosted service and evaluation of a number of other options, MICROS selected Bomgar as it offered a self-hosted collaborative remote support product that provides greater and more direct control over security and PCI compliance concerns.

Bomgar enables MICROS to directly control end-to-end remote access to supported devices as well as physical access to the remote support capability. It gives MICROS direct visibility into remote support, where before this visibility had its limits. When its remote support technology was provided by a third-party service, logs and session records were kept with the service provider and were only available upon request. This also led to concerns about the potential risks of improper handling of these logs, which MICROS felt would have been difficult to mitigate as a customer.

A self-hosted solution gives this control back to MICROS—and more. According to MICROS Chief Information Security Officer (CISO) Jim Walsh, the Bomgar product offers capabilities that not only help MICROS meet security requirements, but also enables them to deliver a higher level of assurance in the support they provide to their customers. For example, it enables MICROS to include its customers in strong authentication to remote support for the customer’s MICROS products. Says Walsh, “Our Remote Access Policy recommends that our customers prohibit remote connection to their MICROS system without their express tactical knowledge and consent.”

“Our Remote Access Policy recommends that our customers prohibit remote connection to their MICROS system without their express tactical knowledge and consent.”

MICROS’s Remote Access Policy recommends that their customers prohibit remote connection to their MICROS system without their express tactical knowledge and consent. The Bomgar product facilitates this policy nicely by permitting access to the customer’s system only after the customer joins our Bomgar session using a link and one-time strong session access credentials that we provide.

---

2 As of April 5, 2011
when services are requested.” The MICROS customer can also constrain access to only the areas that are needed for a specific support task. Access controls are tailored to interface with the MICROS Customer Relationship Management (CRM) system in order to link known identities of MICROS customer personnel with support authorization. Since its initial adoption of the Bomgar product, MICROS has extended its deployment into each of its worldwide operating regions, complete with redundancy in each region.

**EMA Perspective**

The Payment Card Industry Data Security Standard affects more than just the processing of payment card data. As the case described in this paper illustrates, its impact is not limited to retailers alone, but to any business whose interests intersect with the handling of cardholder data. It may also have direct implications for aspects of IT not always identified with the handling of sensitive information, but which can have a significant impact on PCI compliance regardless—such as the technologies required for secure and trustworthy administrative access and remote support.

The PCI DSS stresses the importance of security for high-privilege access to systems that have a direct impact on the cardholder data environment. Remote support technologies must ensure the privacy and confidentiality of highly sensitive access and effectively resist exploit. They must give the enterprise reliable visibility into administrative actions, and provide a comprehensive and “audit-worthy” record of access.

Those that reflect the spirit of the PCI DSS will emphasize security in access, integrity in reporting, and flexible choices for tailoring access to best suit the needs of both the support provider, and the supported customer. Such capability should be considered seriously not just by organizations subject to the PCI DSS, but by any business concerned with meeting the requirements of remote support with solutions that acknowledge the realities of the handling of sensitive information.

**About Bomgar**

Bomgar is a worldwide leader in secure, appliance-based remote support solutions. The company’s award-winning solutions enable organizations to improve IT support efficiency by securely accessing and managing virtually any system – Windows, Mac, Linux, BlackBerry, the iPhone, iPad and most versions of Windows Mobile, regardless of their location. More than 5,500 companies around the world have deployed Bomgar’s enterprise-class solutions to rapidly transform their IT support functions and significantly improve operational efficiency and customer satisfaction while dramatically reducing costs. Bomgar is privately-held with offices in Jackson, Atlanta, San Francisco, Washington D.C., Paris and London. In 2010, Bomgar was named one of the fastest-growing technology companies in America by Deloitte.

For more information please contact Bomgar at pci_info@bomgar.com.
About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2011 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com