

PCI Compliance

The Definitive Guide

Abhay Bhargav



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2014 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed on acid-free paper
Version Date: 20130919

International Standard Book Number-13: 978-1-4398-8740-0 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Bhargav, Abhay.

PCI compliance : the definitive guide / author, Abhay Bhargav.

pages cm

Includes bibliographical references and index.

ISBN 978-1-4398-8740-0 (hardcover : alk. paper)

1. Credit cards--Security measures--Handbooks, manuals, etc. 2. Data protection--Standards--Handbooks, manuals, etc. I. Title. II. Title: Payment-card industry compliance.

HG3755.7.B43 2014

332.1'780681--dc23

2013036711

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

20

Beyond PCI Compliance

An organization begins a journey when it achieves PCI compliance. It is usually a starting point for a continuing path to information security and assurance. It is very important for the organization to understand the potential challenges and effectively address them after they achieve successful PCI compliance. In this chapter, we briefly discuss the challenges and success factors that the organization must be aware of to maintain compliance and achieve optimum information security for the enterprise.

20.1 MAINTAINING PCI COMPLIANCE: THE CHALLENGE

20.1.1 The Challenge: The Dilemma Produced by Success

When the organization achieves PCI compliance, it has achieved success in meeting a highly rigorous and competent security standard. However, this is no indication of success in the future. Information security is not an event, but a process. In this process, there are several challenges that the organization must meet in order to remain secure and compliant. In fact, all too often, I see companies that are PCI certified and compliant be breached by simple attacks that could have been easily prevented if they had maintained their security program and rigor throughout. Also, it is important to remember that security is *not* compliance. Compliance is a by-product of a strong information security program. If a security program of an organization doesn't evolve and improve over time, it is likely to have an adverse impact at some point in the future of the organization. Some of the challenges I see are as follows:

- The information problem
- The technology challenge
- A shift in management attitudes

20.1.1.1 The Information Problem

One of the main challenges in remaining secure and compliant is the information problem. Organizations are very coordinated and orchestrated when they are looking to achieve compliance and certification for the first time. However, after the initial certification and the highs that it provides, they tend to wane on their security program. This is not helped by the fact that assessors and internal auditors also tend to go easy on companies in subsequent assessments and audits. This is primarily caused due to lack of accountability and information. Organizations that have strong security programs have these two traits. They have accountability from a group or an individual for security and compliance. They empower this group/person to make decisions and ensure that the security framework and compliance are met. However, this group or person is accountable for the security program or compliance program. Failing that, there are consequences. This group/person is also responsible for getting the right information, at the right time, from the right people to track the state of security and compliance in the organization. However, I have seen that, more often than not, accountability and information are both sorely lacking for an organization that has achieved information security maturity and PCI compliance and is maintaining the same over time.

The information challenge stems from the fact that information updates that are supposed to be present from different stakeholders are not available or are not available in time. Hence, things get delayed, and security is pushed to the backseat. However, information delivered in time and effectively usually has a way of pushing even the most dormant people into action.

Organizations must look at deploying information-correlation tools like GRC (governance, risk, and compliance) applications, project-management tools, and so on, to maintain tight control over the security and compliance state of the organization on a continuing basis.

20.1.1.2 The Technology Challenge

Technology evolves constantly. Organizations are continually grappling with changes in technology. For instance, cloud computing has become a technology paradigm that most companies seem to want to adopt. However, the migration to such technologies is not well evaluated or researched; hence, organizations somehow forget the security impetus that should be there for their technology initiatives. This creates a scenario that might have serious security implications for an organization. With the extremely dynamic nature of technology change, there are always new vulnerabilities and security flaws being unearthed. For instance, several vulnerabilities have been found on the Web-programming Ruby platform that have rendered several Web applications vulnerable by default, just because of a platform vulnerability.

Organizations that have secured their infrastructure and their technology components cannot afford to take things lightly on a continuing basis. They must stay vigilant to ensure that their security framework takes technology risk into perspective.

20.1.1.3 Management Attitude

I am always receiving complaints about management. Some of them have merit, and some do not. More than 25% of the complainants tell me that management wants

to forget about security once it achieves compliance. They report that there is a great deal of support from management until PCI certification is achieved. However, once the certification is achieved, management automatically believes that the processes are self-sustaining and largely static, with few changes and evolution cycles. This is untrue. Change is constant. The organization's risk might change, technology paradigms might change, the scale and sphere of operations might change, and so on. This requires security frameworks to be constantly reevaluated and improved.

Management must view security and compliance as business enablers and ensure that these enabling functions receive their due by way of resources and allocations to ensure that their business and their critical data are not at risk.

20.2 SUCCESS FACTORS FOR CONTINUING PCI COMPLIANCE

20.2.1 A Change of Attitude

Security is a process, not an event. Organizations must ingrain this philosophy into all their employees. People should view security and compliance as a continuous process that requires consistent maintenance over time, every day, day after day.

20.2.2 Deep Understanding of Risk and Its Application

Most organizations ignore risks to their own peril. It is absolutely essential to evaluate risk regularly (at least annually). PCI

mandates a risk assessment on an annual basis. An annual risk assessment, if done correctly, provides an opportunity to identify and analyze threats that have thus far not been evaluated. Additionally, it provides an opportunity to review existing controls and the effectiveness of these controls. It provides the invaluable opportunity to improve the existing security framework to include a better quality of preventive, detective, and corrective controls.

20.2.3 The CISO

The chief information security officer (CISO) plays a critical role in the organization's security framework. The CISO must be empowered to manage the organization's security framework and practices. Needless to say, the CISO must be one who is well versed in information security practices, technology paradigms, and the organization's business and culture. The CISO must tread a thin line between security and enterprise objectives, ensuring at all times that the organization's security program does not hinder its business objectives and growth prospects.

Also, I have noticed in several organizations that the CISO invariably reports to the CIO or the CTO of a company. This usually engenders a conflict of interest, as these officers are usually in positions of implementation. In such cases, security usually gets lower priority than it requires. The CISO should ideally report to the audit committee or the board. The CISO must also be included in key business and strategy meetings to examine the impact of information security on the organization's initiatives.

20.3 SUMMARY

In this chapter, we briefly explored the factors that could influence the continuing compliance of an organization after it initially achieves PCI compliance. We discussed some of the challenges in maintaining PCI compliance. A significant challenge is the information challenge, where the organization must create accountability and provide information to key stakeholders to effectively manage the organization's security initiatives. We also explored the role of technology change, vulnerabilities, and so on, in the organization's compliance

and security challenges. We learned that management attitudes must address improvement and evolution of the security framework within the organization. Management must not view security as a cost center, but as a business enabler that adds value to the business; hence, it must be improved and evolved as a subsystem within the organization.

Finally, we explored the critical success factors for continuing PCI compliance. Significant factors include a sound understanding and assessment of risk and recognizing the importance of the chief information security officer (CISO) in an organization.