

Achieving PCI DSS, SOX, & HIPAA Compliance through Comprehensive WebSphere MQ Assessments

Identifying middleware security vulnerabilities in today's cyber world

An Evans Resource
Group White Paper

By Maryellen Evans

mevans@evansrg.com



evans
RESOURCE GROUP

Contents

Executive Summary.....	3
Introduction.....	4
Overview of PCI DSS.....	5
SOX and Middleware Data Security.....	9
HIPAA's Security Rule and Its Application to Messaging Middleware.....	11
Conclusion.....	14

Executive Summary

Message oriented middleware is the glue that holds applications and databases together while allowing , and allows for message delivery across the network in today's cyber world. While the current marketplace features numerous providers of messaging middleware, IBM's WebSphere MQ continues to be the acknowledged industry leader with approximately 90 percent market share and over 15,000 installations worldwide.

When IBM created WebSphere MQ in the early '90s, then known as MQSeries, middleware administrators were not overly concerned about security regulations. Rather, they focused on installing and configuring the product in the fastest and most straightforward way they could that would provide the required connectivity for applications, without placing any constraints on usage. As the use of WebSphere MQ grew, it remained common to implement it in an "out of the box" configuration with no security constraints, even though the product provided capabilities for a secure configuration. In addition, personnel responsible for implementing middleware security 15 years ago largely considered WebSphere MQ nothing more than network "plumbing" and utilized assumptions that no longer hold true presently.

Today, message oriented middleware has come out of the shadows of obscurity and into the limelight. As a result of the ubiquitous reach of e-commerce applications and the internet, middleware knowledge has become more prevalent mainstream, including its potential security vulnerabilities and inabilities to meet a growing number of regulatory requirements in today's commercial environment.

The historical result of not implementing security within messaging middleware can lead to potentially severe consequences. As security concerns are now paramount in today's increasingly regulated marketplace, messaging middleware networks are coming under more intense scrutiny. As a result, many companies now stand to fail audits on a variety of regulatory standards requirements that are becoming increasingly more stringent, including PCI DSS, SOX, and HIPAA.

Introduction

As previously stated, the historical result of implementing middleware products such as WebSphere MQ (WMQ) in an “out-of-the-box” manner without security measures, and without knowledge of today’s more stringent regulatory environment, has led to the increased risk of failed audits on a variety of recently enacted regulatory measures. These measures, which were all passed well after the initial growth of messaging middleware, include the Healthcare Insurance Portability & Accountability Act (HIPAA) enacted in 1996, the Sarbanes Oxley Act (SOX), passed in 2002, and the Payment Card Industry Data Security Standard (PCI DDS) enacted in 2006.

As these new regulations were unknown until fairly recently, many companies have not had the time or inclination to invest in securing their middleware, given that they had passed all relevant audits up to this point. The fact that middleware had historically been considered nothing more than network plumbing and as a result was always out of scope of annual security audits, has further contributed to the likelihood of a failed audit.

Today, companies seeking compliance with these new regulatory measures must secure their messaging middleware. However, it has been determined that most current WMQ installations (over 90%) are not configured to properly utilize built-in product functionality that reduces and/or eliminates security threats. Additionally, the default configuration of WebSphere MQ allows anonymous administrative access to the WMQ command server (console), thereby permitting arbitrary remote code execution abilities to unknown users across the network. The implication of these security voids is relatively easy hacking of a layer that is all too often not being adequately protected.

While this security void is applicable to several vendors in the middleware arena, this white paper will focus on IBM’s WebSphere MQ which will provide the only PCI, SOX and HIPAA Compliant messaging middleware solution on the market. The following pages will provide an overview of current regulatory policies, and solutions to help your organization become data security compliant.

Overview of PCI DSS

The **Payment Card Industry Data Security Standard** (PCI DSS) is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC) of which Evans Resource Group is a member. The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. The standard is maintained by the Payment Card Industry Security Standards Council, which maintains both the PCI DSS and a number of other standards, such as the Payment Card Industry PIN Entry Device security requirements (PCI PED) and the Payment Application Data Security Standard (PA-DSS).

Validation of compliance can be performed either internally or externally, depending on the volume of card transactions the organization is handling, but regardless of the size of the organization, compliance must be assessed annually. Organizations handling large volumes of transactions must have their compliance assessed by an independent assessor known as a Qualified Security Assessor (QSA), while companies handling smaller volumes have the option of self-certification via a Self-Assessment Questionnaire (SAQ). In some regions these SAQs still require signoff by a QSA for submission.

Enforcement of compliance is done by the bodies holding relationships with the in-scope organizations. Thus, for organizations processing Visa or MasterCard transactions, compliance is enforced by the organization's acquirer, while organizations handling American Express transactions will deal directly with American Express for the purposes of compliance. In the case of third party suppliers, such as hosting companies who have business relationships with in-scope organizations, enforcement of compliance falls to the in-scope company, as neither the acquirers nor the card brands will have appropriate contractual relationships in place to mandate compliance. Non-compliant companies who maintain a relationship with one or more of the card brands, either directly or through an acquirer, risk losing their ability to process credit card payments, and being audited and/or fined.

PCI Requirements

PCI DSS version 2.0 is the global data security standard adopted by the card brands for all organizations that process, store or transmit cardholder data. It consists of common sense steps that mirror best security practices.

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a <u>firewall</u> configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system <u>passwords</u> and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder 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

PCI DSS originally began as five different programs: Visa Card Information Security Program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and the JCB Data Security Program. Each company's intentions were roughly similar: to create an additional level of protection for customers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data. The Payment Card Industry Security Standards Council (PCI SSC) was formed, and on December 15th, 2004, these companies aligned their individual policies and released the Payment Card Industry Data Security Standard (PCI DSS). In September 2006, the PCI standard was updated to version 1.1 to provide clarification and minor revisions to version 1.0. Version 2.0 was released in January of 2011.

PCI Controversies and Exposures

It is suggested by some IT security professionals that the PCI DSS does little more than provide a minimal baseline for security. They point to the fact that some companies have had security breaches while being registered as PCI DSS compliant. In 2008, one of the largest payment service providers, Heartland Payment Processing Systems, suffered a data breach which has been estimated by some as exceeding one hundred million card numbers. Other notable breaches include those of Hannaford Brothers and the Okemo Mountain Resort, each of which was previously proclaimed PCI compliant.

It has been noted that this may be an indication of the limits of a snapshot certification; i.e., the evaluation cannot ensure that the target company will maintain the good practices seen in an audit. However, this explanation does not seem to adequately explain certain instances of compromise to merchants such as Hannaford Brothers Company, which received its PCI DSS compliance certification one day after it had been made aware of a two-month long compromise of its internal systems.

The definition of *compliant* has also been open to interpretation, especially regarding how temporary such a declaration might be. Declaring a company *compliant* appears to have some temporal persistence, yet the PCI Standards Council General Manager, Bob Russo, indicates that liabilities could change depending on the state of a given organization at the point in time when an actual breach occurs. Similar to other industries, a secure state could be more costly to some organizations than accepting and managing the risk of confidentiality breaches. However, many studies have shown that this cost is justifiable.

So what is the bottom line related to non-compliance of PCI DSS? Card companies like American Express, VISA, MasterCard, JBC, and Discover may impose fines on their member banking institutions when merchants are found to be non-compliant. In addition, acquiring banks may in turn contractually oblige merchants to indemnify and reimburse them for such fines. Fines could go up to \$500,000 per incident if data is compromised and merchants are found to be non-compliant. In the worst case scenario, merchants could also risk losing the ability to process customers' credit card transactions.

Businesses from which cardholder data has been compromised are also obligated to notify legal authorities and are expected to offer credit-protection services to those potentially impacted. Cardholder data loss, whether accidental or through theft, may also lead to legal action being taken by cardholders. Such a step will result in bad publicity, which may in turn lead to loss of business.

SOX and Middleware Data Security

Compliance with the U.S. Public Company Accounting Reform and Investor Protection Act of 2002 (the Sarbanes-Oxley Act or SOX) requires that Information Systems (IS) organizations work with other departments – mostly finance and legal – in almost-unprecedented ways. However, a recent Gartner survey conducted with 75 senior regulatory compliance managers at U.S.-based public companies revealed that this is not happening.

This apparent lack of IS department involvement is alarming for several reasons. Financial documentation and controls are heavily dependent on Information Technology (IT) systems. If IT systems are not being included in the audit process, there is a risk that companies will not be Sarbanes-Oxley-compliant. The Big Four auditing firms, on which most large companies are relying to help them through the compliance process, are recommending the use of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Risk Management Framework. This document is designed to instill "risk and control consciousness," and is a model for discussing and comparing risk management and internal controls. The COSO Framework contains specific IT-related advice. It is therefore surprising that the financial personnel who are driving the Sarbanes-Oxley efforts within their companies have not, in every case, involved their IS departments in the compliance process.

This trend is especially disturbing when one considers that one of the key requirements of SOX is that executives are required to certify, under penalty of law, that their financial data are true and accurate.

However, given the above, it's apparent that the focus has been on certifying that the aggregate financial data are true and accurate, not the actual transactions from which revenue flows. Imagine if it was common practice to let anybody in the company, from the CEO to the maintenance and housekeeping staff, access, modify and update customer transactions? Would it be accurate then to say that there were sufficient controls and accountability to satisfy SOX? Most would say definitely not. Yet, this is the situation that we at Evans Resource Group encounter in the vast majority of cases in our roles as WebSphere security consultants.

Although WebSphere Application Server and MQ can be configured to restrict administrative access, in most cases, it is not. The result is that anyone with an IP route to the queue manager (a queue manager is a running instance of

WebSphere MQ) can anonymously connect and access any message flowing through the system, delete messages, update them or inject rogue messages into the system. This situation is what we usually find when performing security assessments. The queue manager is completely exposed to the entire intranet. Occasionally we find an installation where anonymous connections have been restricted. In nearly all of those cases though, legitimate users and applications are granted administrative access. This still falls far short of what would be considered effective internal controls. In addition, WebSphere MQ provides its administrators a function to remotely execute commands on the MQ host server. When ordinary users and applications are inappropriately granted administrative access, they inherit this remote code execution capability on the servers which host the company's most critical business applications.

There are a number of factors which give rise to and perpetuate this problem. Primary among these is that WebSphere MQ security is not well understood. By default, a remote connection will pass the user's local ID to the queue manager for authorization. This is widely used as the basis for very granular and often complex security models. What is not commonly known, however, is that the user can optionally choose to pass in any arbitrary ID, including an administrative one. WebSphere MQ can be configured to authenticate these IDs that are passed in but usually it is not.

Due to the fact that the ID passed in appears to have been authenticated, there is a general misconception that it has been and can be trusted. In fact, the exact opposite is true. The result is that the companies most exposed are usually the ones that are most confident in their WebSphere security. They certify the veracity of their financial data simply because they don't know any better.

As a result, our initial recommendations regarding messaging middleware security and SOC compliance focus on education of applicable IS departments and their duties if they are not now involved in Sarbanes-Oxley compliance processes. More specifically, we strive to increase awareness that:

- Messaging middleware is now a strategic target of hackers
- Trillions of dollars of transactions flow through messaging middleware each week
- Administrative access to messaging middleware is a SEV-1 finding on a data security audit.
- Information System departments must have a major role in compliance.
- Established systems must be audited and tested as per Section 404. CIO

If you are one of the executives who signs off on the SOX certification for your company, it's time to check your messaging network. If security has not been enabled correctly, the SOX certification may not be worth the paper it's written on.

HIPAA's Security Rule and Its Application to Messaging Middleware

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. According to the Centers for Medicare and Medicaid Services (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. This is intended to help people keep their information private, though in practice it is normal for providers and health insurance plans to require the waiver of HIPAA rights as a condition of service.

The Administration Simplification provisions also address the security and privacy of health data. The provisions are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

HIPAA's Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans". The Security Rule complements the HIPAA Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications.

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, widens the scope and security protections under HIPAA; increases potential legal liability for non-compliance; and provides more enforcement of HIPAA rule. It imposes notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities in the

event of certain security breaches relating to protected health information (PHI).
The standards and specifications are as follows:

- **Administrative Safeguards** – policies and procedures designed to clearly show how the entity will comply with the act
 - Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
 - The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
 - *Procedures should clearly identify employees or classes of employees who will have access to electronic protected health information (EPHI). Access to EPHI must be restricted to only those employees who have a need for it to complete their job function.*

NOTE: This requirement calls for the separation of duties within the development and production environments within messaging middleware.

- *The procedures must address access authorization, establishment, modification, and termination.*

NOTE: This requirement addresses data at rest.

- Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to employees performing health plan administrative functions.
- Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
- A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

- **Technical Safeguards** – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.
 - Information Systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
 - Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
 - Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
 - Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems.
 - Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
 - In addition to policies and procedures and access records, Information Technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
 - Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)
- **Enforcement Rule**
 On February 16, 2006, HHS issued the Final Rule regarding HIPAA enforcement. It became effective on March 16, 2006. **The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations;** however, its deterrent effects seem to be negligible with few prosecutions for violations to date.

Conclusions

Current security assessments and related protocols are not addressing a known pervasive vulnerability associated with the installation and maintenance of IBM's WebSphere MQ (WMQ) and other middleware. IBM's WMQ accounts for 87% of messaging oriented middleware software that is within 75% of the Fortune 100. There are currently 15,000 WMQ users globally and WMQ is embedded in all major WebSphere products used by the government, finance, banking, retail, and other major industries. Mis-configuration or non-configuration of WMQ leads to unauthorized administrative access which is a critical infrastructure vulnerability that allows hackers to own the system. Ninety percent of WMQ penetration testing done by ERG has failed to meet the requirements for basic data security including confidentiality, integrity and accessibility.

Penetration testing and configuration assessment are the industry roadmaps to understand network vulnerability. However, middleware assessments and penetration tests do not use the same technology as perimeter-based methods. Vulnerabilities that are due to mis-configuration and non-configuration of middleware have to be tested "within context". A scan of the perimeter will provide no relevant information regarding middleware security since it is not familiar with the complex configurations for security that are required.

As with other potential threats to data security, protection of the WebSphere MQ network requires organizations to apply security using a phased approach. When looking at any proposed solution, it is important to understand the following criteria:

- Types of threats, in depth
- Impact on customer experience
- Future growth of the WMQ network

The application of security exits will ensure an appropriate level of compliance at each segment of the WMQ network, assuring that administrative, application and data requirements are met. These levels can be triaged by setting appropriate parameters, upgrading to the appropriate versions across platforms and providing authentication with tools such as SSL or WebSphere Advanced Message Security (AMS) where appropriate.

To further safeguard against potential non-compliance, it should be noted that applying only one level of security will not be sufficient. Adding risk-based, multi-level authentication and authorization based on role and responsibility will provide more robust protection against exposures as well as alignment with required compliance standards to successfully pass PCI DSS, SOX and HIPAA audits.

ABOUT EVANS RESOURCE GROUP

Evans Resource Group can secure the WebSphere MQ network for merchants, acquiring banks, processors, healthcare and public enterprises that are among the more than 15,000 organizations in 60 countries using MQ today. Leveraging a program of assessment and remediation, constructed in conjunction with IBM's WebSphere Security team, we provide a multi-phased approach to data security that addresses growing risks using our WebSphereSentry program and product. For information, call 212.937.8443 or email info@evansrg.com or visit www.evansresourcegroup.com

This White Paper is for informational purposes only. EVANS RESOURCE GROUP (ERG) MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS WHITE PAPER. ERG cannot be responsible for errors in typography or photography.

All brand, company, and product names referenced herein are used for identification purposes only and may be trademarks or registered trademarks of their respective owners.

©Copyright 2011 Evans Resource Group. All rights reserved. Reproduction in any manner whatsoever without the express written permission of Evans Resource Group is strictly forbidden. .

Information in this document is subject to change without notice.