

“Mapping Sarbanes-Oxley to Payment Card Industry Standards”

Pat Slagle, PMP & Cris DeWitt, CISSP

OVERVIEW	1
SARBANES-OXLEY IT CONTROL OBJECTIVES.....	1
AMERICAN EXPRESS DATA SECURITY REQUIREMENTS.....	3
SARBANES-OXLEY/PAYMENT CARD INDUSTRY SECURITY STANDARDS MAP	4

Overview

Identity theft and credit card fraud has become very big business. Recently, US government security agencies disbanded an online 4,000- member organized crime syndicate for trafficking in stolen credit cards, goods, and falsified documents¹. Other heavily publicized incidents related to hacking, theft or loss of confidential personal information demonstrates the potential for significant financial losses and a negative impact on consumer confidence. These include:

- Bank of America’s loss of approximately 1.2 million government charge card holder account files in December of 2004².
- As reported in May of 2005, Harvard University Credit Union lost approximately 700 credit card accounts, which included CEO Eugene Foley’s information that resulted in a personal loss to him of over \$2000.00³.
- Polo Ralph Lauren’s loss by theft of approximately 180,000 card holder’s account information in April of 2005⁴

Considering the large number of credit card transactions that occur daily, face to face and electronically, the risk of financial loss is high. To reduce this risk, credit card companies like Visa, MasterCard and American Express, have instituted information security standards (CISP – Cardholder Information Security Program, AMEX Data Security Requirements) that companies must adhere to in order to maintain good standing with the credit card companies and to avoid fines or even loss of service. Combine these requirements with the stringent Sarbanes-Oxley governmental regulations, and companies must expend significant effort to meet these multiple requirements. To help demystify this myriad of requirements, In-Depth Security has developed a tool that maps the control objectives from Sarbanes-Oxley⁵ with those of Visa/MasterCard⁶ and American Express⁷.

NOTE: This complimentary paper includes the Overview, IT Control Objectives and a sample page of the tool/map. To receive this valuable 17 page report in its entirety; please call Doug Jarosh of In-Depth Security at 512-263-8240, ext. 205, to arrange for delivery.

¹ Baseline Magazine, 3/14/2005 "Geekfathers: CyberCrime Mobs Revealed"

² <http://financialservices.house.gov/media/pdf/050405bd.pdf>

³ <http://financialservices.house.gov/media/pdf/050405ef.pdf>

⁴ <http://msnbc.msn.com/id/7501064/>

⁵ "IT Control Objectives for Sarbanes-Oxley", April 2004, © IT Governance Institute

⁶ "Payment Card Industry Standards", Version 1.0 December 2004, © Visa

⁷ American Express Data Security Requirements (website), © 2004, American Express

Sarbanes-Oxley IT Control Objectives

IT General Controls—Program Development and Program Change

S1 -Acquire or Develop Application Software

Control Objective—Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.

S2 - Acquire Technology Infrastructure

Control Objective—Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support financial reporting applications.

S3 - Develop and Maintain Policies and Procedures

Control Objective—Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.

S4 - Install and Test Application Software and Technology Infrastructure

Control Objective—Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and associated controls operate as intended and support financial reporting requirements.

S5 - Manage Changes

Control Objective—Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.

IT General Controls—Computer Operations and Access to Programs and Data

S6 - Define and manage service levels

Control Objective—Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies financial reporting system requirements and provides a common understanding of performance levels with which the quality of services will be measured.

S7 - Manage third-party services

Control Objective—Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and defined appropriately in performance contracts.

S8 - Ensure systems security

Control Objective—Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

S9 - Manage the configuration

Control Objective—Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

S10 - Manage problems and incidents

Control Objective—Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.

S11 - Manage data

Control Objective—Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.

S12 - Manage operations

Control Objective—Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.

American Express Data Security Requirements⁸

General Security Requirements

Disclosure

A1 - Establish a company privacy policy that explains the security measures your company has put in place to protect Cardmember transaction data.

Firewalls

A2 - Employ internal and external firewalls to prevent intrusions from the internet and from within your own organization.

Encryption

A3 - Encrypt all stored payment data using triple DES encryption.*

Employee access/Passwords

A4 - Assign employee access to payment data on a need-to-know basis.

A5 - Assign a unique ID to each person with computer access to payment data.

A6 - Maintain the ability to track employee access to payment data through the use of unique IDs.

A7 - Change employee Passwords regularly.

A8 - Ensure employee security policy is understood by all your employees.

A9 - Require two-person control to access encrypted data.

Systems

A10 - Routinely test internal security systems and processes. Quarterly certification of systems and processes by a third-party Security Evaluation Company is preferred.

A11 - Maintain physical building and premise-access security.

A12 - Restrict physical access to Cardmember payment data.

Audits

A13 - Be prepared to provide audit reports to American Express or allow American Express audits.

A14 - Never store payment data on a web server or cache anywhere in memory related to a web server. Payment data may only be stored in a separate, secure database, with at least one external firewall.

A15 - Never store Card Identification (CID) information. (A CID may be maintained on your systems only to obtain authorization, in order to process a Cardmember payment.)

A16 - Never use Cardmember payment data for any purpose other than processing future transactions.

A17 - Never store track data from the magnetic stripe on the back of the Card.

A18 - If you store American Express[®] payment information, you are obligated to notify us immediately if that data is (or may have been) compromised. In addition, you're expected to act in good faith and work with American Express to rectify any issues that may result from this activity.

Online Transaction Requirements

Infrastructure Requirements

A19 - Website must be enabled with Secure Socket Layer 3.0, with 128-bit encryption.

A20 - American Express-certified POS device and/or methodology should be used to transmit all transaction information to American Express.

A21 - Every online transaction must be authorized using a unique Internet SE number and appropriate POS Data Code.

Authentication Requirements

A22 - Establish time limits for consumer sessions.

A23 - Prevent customer access to secure data, following three failed log-on attempts.

A24 - Establish safeguards to prevent employee access to Cardmember Passwords.

⁸ American Express Data Security Requirements (website), © 2004, American Express

A25 - Set up administrative authority for resetting Passwords, issuing temporary Passwords, and accessing payment information by restricting access to authorized employee groups and enabling the creation of audit trails.

A26 - Monitor/track access and usage reporting.

Transaction Security and Privacy

Storage of Cardholder Info

Do not store the following under any circumstance.

A27 - Full contents of any track from the magnetic stripe on the back of the card.

A28 - Card-validation code--the three-digit value printed on the signature panel of a MasterCard®, Visa®, Discover®Card, JCB®, or Diners Club® card, and four-digit code printed on the front of an American Express® card.

A29 - Store only that portion of the customer's account information that is essential to your business--i.e. name, account number or expiration date. Store all material containing this information (e.g., authorization logs, transaction reports, transaction receipts, car rental agreements, and carbons) in a secure area limited to authorized personnel. Destroy or purge all media containing obsolete transaction data with cardholder information.

Use of agents or 3d parties

A30 - Advise each merchant bank or processing contact (representing each of your card brands) of any agents that engage in, or propose to engage in, the processing or storage of transaction data on your behalf--regardless of the manner or duration of such activities.

A31 - Make sure these agents adhere to all rules and regulations governing cardholder information security. Any violation by your agent may result in unnecessary financial exposure and inconvenience to your business.

Reporting a Security Incident

A32 - In the event that transaction data is accessed or retrieved by any unauthorized entity, notify the merchant bank or processing contact for each card brand immediately.

Record of Charge Truncation

A33 - no person accepting credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of sale or transaction

PCI Data Standard (CISP)	AMEX Data Security Requirements	SOX IT Controls											
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12
Requirement 1: Install and maintain a firewall configuration to protect data.			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
1.1 Establish firewall configuration standards that include:	A2			✓									
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration.				✓			✓		✓	✓			✓
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks.						✓				✓			
1.1.3 Requirements for a firewall at each Internet connection and between any DMZ and the Intranet.			✓					✓	✓				
1.1.4 Description of groups, roles, and responsibilities for logical management of network components.			✓										
1.1.5 Documented list of services/ports necessary for business.			✓							✓			
1.1.6 Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN.			✓							✓			
1.1.7 Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented.			✓		✓			✓	✓				
1.1.8 Periodic review of firewall/router rule sets.								✓	✓				
1.1.9 Configuration standards for routers.			✓			✓							
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, except for:								✓					
1.2.1 Web protocols - HTTP (port 80) and Secure Sockets Layer (SSL) (typically port 443).								✓					
1.2.2 System administration protocols (e.g., Secure Shell (SSH) or Virtual Private Network (VPN)).								✓					
1.2.3 Other protocols required by the business (e.g., for ISO 8583).	~A20												
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:								✓	✓				
1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters).								✓	✓				
1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443.								✓	✓				

Please call Doug Jarosh at 512-283-8240, ext. 205 to receive your free copy of this 17 page white paper in its entirety.