

Section A – Cover Page

2008 NASCIO Award Submission

**Utilizing PCI Compliance to Improve Enterprise Risk
Management**



Information Security and Privacy
Michigan

Section B - Executive Summary

Michigan has implemented a citizen centric portal that supports over 970 e-government services from filing unemployment claims on-line to renewing automobile license plates. One of the common requirements across many of these services is the need to provide payment for services via credit cards. While payment via credit card is an advantage for the citizen and the State, it does increase the risk of a security breach from cyber criminals who are making concerted efforts to harvest personal identity information from Internet based systems.

Michigan on average has seen an annual attack rate of 194 million attempts against its critical IT infrastructure. Many of these attacks if not stopped would result in data breaches. In 2007, a study done by Ponemon Institute estimated that the average cost of a data breach was \$187 per breached customer record¹. For States that have millions of pieces of personal information a breach would not only be expensive in terms of the unbudgeted cost to respond and remediate but would also greatly affect the confidence of users of on-line services. The MDIT's Office of Enterprise Security estimated that the cost of breaches to one of Michigan's critical systems could cost the state as much as \$35 million dollars.

In an effort to reduce the risk of data breach caused by such attacks, the credit card industry created the Payment Card Industry Data Security Standard (PCI). The industry requires merchants and credit card payment providers to validate their compliancy with the standard on a periodic basis or face substantial fines or loss of the ability to process credit card transactions.

The Michigan Department of Treasury, which is responsible for managing the state's credit card relationship, and the Michigan Department of Information Technology (MDIT), which is responsible for the State's information technology, joined forces to develop processes and procedures to ensure that Michigan's Internet based systems would remain PCI compliant. The MDIT used the joint project as a means to consolidate and strengthen its change management process; add security compliance to its development life cycle; implement a security exception process; increase security awareness of its application and technical staff; close audit findings; close security holes identified in an external penetration test; meet the payment card industry security requirements; implement best practices; and satisfy its customer, Treasury.

The PCI standard has actually become a central catalyst around which Michigan's overall risk management strategy has been organized. By adopting the PCI standard as a best practice and aligning its security measures with Michigan's business processes, Michigan has seen significant benefits not only to taxpayers but to agencies at a time when state budgets are more than just a little tight. The MDIT Office of Enterprise Security believes that public institutions could benefit greatly by implement PCI as the foundation of their risk management process.

Therefore, this PCI compliance project provides a best-practice approach that is transferable to governments of any size with repeatable improvements for people, processes and technology. Not only has this project enabled protection of credit card transactions, but it will increase citizen trust and diminish the likelihood of identity theft or the loss of any type of sensitive data. The critical IT infrastructure in Michigan has been strengthened – enabling citizens-centric web solutions.

¹ Ponemon Institute's Annual Study: Cost of a Data Breach

Section C - Description

Data Breaches a major risk in offering e-government services - The State of Michigan has been expanding its e-government presence on the Internet since the late 1990s. With this expansion has come the business need to offer citizens the convenience of paying for services electronically using credit cards. The problem facing Michigan was how to reduce the risk of possible data breaches, improve processes, gain better control over its e-government infrastructure and at the same time demonstrates compliance with a control security framework to state and federal auditors.

Michigan Departments join forces to implement PCI standard - In 2005, the Michigan Departments of Treasury and Information Technology (MDIT) joined forces to reduce the risk of data breaches to personal information by implementing the Payment Card Industry Data Security Standards (PCI). These security standards have a broad range of requirements for controls and monitoring procedures to safeguard personal identifying information and included the PCI “dirty dozen”:

- Installing and maintaining a firewall configuration to protect cardholder data
- Not using vendor-supplied defaults for system passwords
- Protecting stored cardholder data
- Encrypting transmission of data across open/public networks
- Using and updating anti-virus software
- Developing and maintaining secure systems and applications
- Restricting access to cardholder data to a need-to-know basis
- Assigning a unique ID to each person with computer access
- Restricting physical access to cardholder data
- Tracking and monitoring access to network resources
- Regularly testing security systems and processes
- Maintaining a policy focused on information security

The State could have faced a number of different costs should a data breach occur and its networks were not compliant. These costs could include: fines of up to \$500,000/incident; victim notification costs; replacement card costs; costs associated with the fraudulent transactions; identity theft Insurance for victims and the costs for performing forensics. In addition the state’s acquirer could refuse to process credit card payments which would limit the usefulness of a number of services provided on-line to citizens, forcing citizens back into lines at state offices.

At approximately the same time the MDIT via the Office of Enterprise Security (OES) had started a project to remediate vulnerabilities found in the State’s demilitarized zone, as a result of a penetration test. Combining the two projects made a lot of sense.

Barriers and Challenges - There were a number of barriers and challenges that the project faced:

- A poorly administered change control for infrastructure move, add, change – at best, MDIT had multiple change processes and in most cases no change control process. This allows self-inflicted problems to be introduced into the infrastructure supporting credit card transactions.

- Negative penetration test results, audit findings – a penetration test completed in the spring of 2005 and a number of IT audits showed a number of weaknesses in MDIT’s infrastructure security and control processes.
- Lack of sense of urgency on the part of technical and systems staff to change – IT staff were busy during this time period on competing projects and did not see the value of implementing new processes that “would slow down” the process of implementing new systems.
- Culture and attitude hurdles – Many technical and systems staff felt that they owned the servers and applications and had been managing them for years, and the attitude of “don’t touch my server, we’re different” prevailed.
- Skill sets training for technical staff lacking – a considerable number staff demonstrated during the pen test remediation that they lacked skills in resolving vulnerabilities.
- Multiple tool sets – MDIT used a number of tool sets to determine vulnerability compliance. This resulted in the inability to have a true enterprise picture of vulnerabilities. In addition none of the tools sets were qualified to determine PCI compliance.
- Constantly changing vulnerabilities and requirement targets – During the pen test remediation project it was hard to gauge how much progress remediation teams were making because the number of vulnerabilities change constantly.

The Solution

Establish a PCI Compliance Board - a compliance board was established for the expressed purpose of monitoring the progress made towards PCI compliance. This board is comprised of Treasury and MDIT staffs who meet monthly to monitor the continuance PCI compliance of the State’s network.

Executive level Buy-In – The compliance board gained executive level support from both the State Treasurer and the State Chief Information Officer (CIO)². This support gave the project the priority it needed it needed to get implemented.

Briefings for MDIT Management Staff – In order to overcome culture and communication hurdles demonstrated by technical and systems staff during the pen test remediation project, the project team held briefings for all MDIT management levels. These briefings explained what was meant by PCI compliance; the importance of the project; project expectations; and demonstrated executive level support for the project.

PCI Compliance Scanning Service – One of the requirements of PCI is that all Internet facing devices must pass a network scan performed by an Approved Scanning Vendor (ASV). The State selected Qualys as its ASV and subscribes to their QualysGuard Enterprise service. The service automates the process of vulnerability management and PCI policy compliance by providing network discovery and mapping, asset prioritization, vulnerability assessment reporting and remediation tracking according to business risk. The PCI policy compliance feature allows the State’s PCI Compliance Board to audit, enforce and document compliance with PCI. It allows infrastructure and application teams to receive detailed vulnerability scan reports by IP asset that can be used to resolve vulnerabilities.

² The State Treasurer is the Department Director for the Department of Treasury and the CIO is Department Director for the Department of Information Technology.

Michigan's QualysGuard Enterprise Implementation – The OES manages the QualysGuard service and has implemented the use of the service in three ways. First, a department wide change management process was implemented. As part of that process, any device in the state's network must pass a PCI compliant vulnerability scan before it is added to the network or before a configuration changed can be made. Second, OES runs monthly scans of all Internet facing devices and any backend services that connect to these devices. The detailed scan results are sent to application owners who work together with infrastructure teams to remediate the vulnerabilities. OES then summarizes the results and inputs them into a Vulnerability Scanning Scorecard that is given monthly to MDIT's executive team and the PCI Compliance Board. Third, OES staff have trained members of IT infrastructure teams in the use of the Qualys scanning tool so they could perform intermediate scans. This allows teams the ability to verify that devices have been remediated successfully prior to going through the change management process.

MDIT Executive Management Review – The MDIT executive management team monitors progress of the project by reviewing a monthly PCI compliance score card. The score card shows the remediation progress by customer and allows the executive team to adjust a team's work load if needed.

Length of time in operation – The PCI compliance process has been in operation since June of 2006.

Baseline and changes in metrics – When this project started there were 318 significant vulnerabilities in devices that were Internet facing. As of May 2008, there were no vulnerabilities in the State's DMZ (demilitarized zone).

Leverage and Transferability - The process that the State of Michigan uses for PCI compliance can be transferred to any government or private organization. The state is currently rolling out this same process to local units of government in Michigan.

Section D - Significance

Scope of the project – prior to the implementation of the PCI project, security compliance was addressed on a project-by-project basis within each of the 19 Executive Branch agencies in Michigan. The project succeeded in implementing a single enterprise security risk management foundation across the state.

Policy alignment – The PCI compliance program directly supports two of Governor Jennifer M. Granholm's five priorities for the state:³ Better Government and Safe Places to Live and Work for All of Us. The program is also aligned with MDIT's department goals: “operations, security and reliability through statewide solutions and universal standards”; expanding “Michigan's services to reach citizens and business anytime, anywhere”; “drive[ing] innovative processes and technologies to transform Michigan's government service”. The project is a major focus of Office of Enterprise Security's strategic plan.⁴

³ 2008 State of the State Priorities: Education for Every Child/Training for Every Worker, A Job For Every Worker, Better Government, Safe Places to Live and Work for All of Us and Health.

⁴ See MDIT Strategic Plan, http://www.michigan.gov/documents/itstrategicplan/C_StrategiesTargets_Web_234548_7.pdf

Beneficiary groups - The beneficiaries of Michigan's PCI compliance process can be broken into two groups; internal to state government and external to state government. The internal beneficiaries are the 19 Executive Branch agencies. This group includes the departments of: Agriculture, Civil Rights, Civil Service, Community Health, Corrections, Education, Environmental Quality, History, Arts and Libraries, Human Services, Information Technology, Labor & Economic Growth, Management and Budget, Military & Veterans Affairs, Natural Resources, Secretary of State, State Police, Transportation and Treasury.

Since 2006, the PCI compliance program has been the supporting foundation on which Michigan has built its e-government services. These services support a wide range of external beneficiaries including businesses as customers, as partners, and as taxpayers, and citizens as service customers and as taxpayers.

Project Impact - Most people are familiar with the benefits that e-government services offer; Responsive, Transparent and Accountable, Accessible, Responsible, Efficient and Effective, Participatory. The PCI compliance project cements these benefits together by reducing the risk of data breach and thus increasing constituent trust in the service. Trust is the foundation on which e-government relationships between constituents and the state are built. As trust grows it leads to more constituent use of services, a cost reduction and a time savings for all. On the other hand, a data breach would have the opposite effect. It would reduce use and increase cost to all. As a result, the importance of having secured e-government services and the importance of the PCI compliance project can not be understated. Michigan now offers 970 e-government services via its state portal and is in the process of developing additional services all built around PCI security.

Section E – Benefit of Project

Project Benefits – The PCI compliance program as implement in Michigan has the following benefits⁵:

- *E-government business success/resilience [internal]*. Though the implementation of an enterprise change management function and regular scanning of Internet assets, the PCI compliance program has allowed state agencies to carry out their missions by focusing MDIT's attention on the confidentiality, integrity, and availability of strategic citizen services.
- *Performance improvements and more effective financial management [internal]*. Part of the PCI compliance program was inserting security into the systems development life cycle, SUITE (State Unified Information Technology Environment).⁶ This allowed for both performance gains and financial savings by implementing security controls before systems became operational rather than after it has gone operational; after an audit; or, worst case, after a security incident or breach.
- *Security is integrated within agency business processes [internal]* – MDIT has used the PCI program to proactively deploy security to all agency operations. The security controls provided by the PCI in turn have enabled agencies to deliver enhanced web based e-government applications to citizens to fulfill their missions.

⁵ Which beneficiary group the benefit applies is noted in brackets. See previous page for beneficiary groups.

⁶ <http://www.michigan.gov/suite>

- *Transparency in oversight [internal]* – Implementing the PCI compliance process has brought transparency to the many different levels of IT oversight that state agencies and the MDIT must work through. Having a well-defined standard and toolset that can be mapped to different compliancy standards allows operational groups both with state agencies and MDIT to reduce the time spent reviewing and gathering information required by various internal and external auditors.
- *Risk management is becoming an integral part of doing business [internal]*. The principal goal of MDIT’s risk management process is to protect a state agency’s ability to perform its mission. Prior to PCI this was treated as technical function at best. With the implementation of PCI compliance agencies are treating it as an essential management function as they develop new e-government services.
- *Increased availability of e-government services[external]* - PCI compliance makes security a priority for delivery of an e-government service. This improves the availability and integrity of the service. This also allows a citizen to renew their driver license, get a state income tax form, look up unclaimed property, register for a permit, or file for unemployment (to name a few) at their leisure based on their schedule and not on government’s schedule. This makes government available to citizens on a 24 x 7.
- *More available e-government services* – Having an enterprise-wide PCI compliance program builds customer confidence that services can be trusted to keep their personal and business data private and secure. Secure services lead to more services being developed which then lead to lower cost government.
- *Improved use of resources* - Improves the productivity of system administrators who are responsible for vulnerability remediation

Operational Savings – Although security ROI can sometimes be difficult to identify, the following calculation exhibits the anticipated benefits for Michigan taxpayers.

\$35 Million in Savings

The project team used two sources of information to determine likely savings should a data breach occur. The first was Ponemon Institute’s Annual Study: Cost of a Data Breach and the second was Privacy Rights Clearinghouse. Ponemon’s study showed that the average cost of a data breach was \$197 per customer record breached in 2007 and \$182 for a breach in 2006. The second source of information was the Privacy Rights Clearinghouse’s A Chronology of Data Breaches. This lists all data breaches that have been reported since 1995 and lists the number of customer records breached. The project team used the number of records breached for each state that had data a breach caused by network hacking and determined the average number of customer records breached per incident. That average number was 183,023 per incident. The third source of information was Michigan’s cyber security attack metrics for 2007 (16,850,239) and 2006 (22,038,058).

The formula for savings was determined as follows:

- FY2006 Savings \$33,310,186.00 = \$182*183,023
- FY2007 Savings \$36,055,531.00 = \$197* 183,023
- Average Annual Savings of \$34,682,858.50 = (\$33,310,186.00+\$36,055,531.00)/2
- Average Annual Attacks = 194,4148.5 (16,860,239+22,038,058)/2