1. Nomination Form Information:

Category:	Information Security and Privacy
Title of Nomination	Security 2.0: Next Generation Security Program
Project Manager:	Dan Lohrmann
Job Title:	Michigan Chief Information Security Officer
Agency:	Office of Enterprise Security
Department:	Michigan Department of Information Technology
Address:	515 Westshire Drive
City:	Lansing
State:	Michigan
Zip:	48913
Phone:	(517) 241-4090
Fax:	(517) 241-2013
Email:	LohrmannD@Michigan.gov

2. Executive Summary

The Internet has changed everything, including government opportunities to proactively serve the public in new, innovative ways. Not only have Michigan citizens come to expect secure e-government transactions and ease of use on a 7 x 24 x 365 basis, the public is now calling for a new generation of "Web 2.0" transactions with a new level of collaboration. From MySpace to Google to YouTube, Michigan is forging ahead to provide new services and communication techniques that utilize new technologies. Two essential keys to success are ensuring that we move forward in a secure manner that addresses the serious challenges that come with these new technologies, while at the same time addressing traditional cyber threats posed by the Internet and other security risks.

One study done this year by a local consulting firm showed that Michigan citizens fear identity theft more than they fear the loss of a job, home foreclosure or a terrorist attack. Therefore, our "Security 2.0" program is addressing these fears by placing cyber protection at the top of the priority list as we move forward with infrastructure enhancements for Web 2.0 applications.

With the goal of strengthening the central policymaking and direction-setting in all areas of information technology, including security and data protection, Michigan's Department of Information Technology (DIT) was formed in 2002. Our initial (1.0) Secure Michigan Initiative Program improved the availability, confidentiality and integrity of Michigan systems and at the same time ensured that newly added e-government services were also protected.

Michigan's Security 2.0: Next Generation Security Program was started three years ago to deal with the changing Internet threat profile identified by the Office of Enterprise Security (OES). This program encompassed 15 projects that were planned in 2004 and implemented between 2005 and 2007. The project supported the following initiatives: Enterprise Filtering Initiatives, Vulnerability Assessment Initiatives and Security and Readiness Response initiatives.

Through a defense-in-depth architecture, Michigan now mitigates a number of the major Internet risks associated with offering services over the Internet. A large portion (over $5 million) of this program was also funded with Homeland Security dollars.

This program has already had many positive benefits to both government operations and the public. It protected the network from over 91 million viruses last year. This effort reduced the amount of hardware and software necessary to operate the e-mail system. It protected the amount of network bandwidth available for state operations. The program greatly reduced the number of field service calls made to remove malware from state workstations. This allowed DIT to reduce its IT support costs. It prevented 11.4 million attempts to deface public websites which could have had a disastrous effect on the state's reputation. It eliminated over 3.2 million Internet browser based compromises which could have affected the operation many critical state programs.

The Security 2.0: Next Generation Security Program has not only had a positive impact on securing Michigan's technology infrastructure, this program has yielded an annual return on investment of over $10.7 million. Even more importantly, legislators and senior executive leaders in the state have praised this program as being innovative and timely.

Governments who are thinking of offering secure e-government services should consider reviewing Michigan's security program. Whether an organization is small or large, a local or a state government, or a K-12 school or university, there are elements in Michigan's 2.0 security program that can be used to address their internet fears.

3. Justification

A. Project Description

A New World

Consolidated IT Environment - In 2001, Michigan consolidated the information technology assets of twenty-one executive branch departments. This action brought together 50,000 plus workstations, 3,000 servers, hundreds of communications and approximately 1,700 employees/contractors under the management of a single Department of Information Technology (DIT). The goal of the new department was to strengthen central policymaking and direction-setting in all areas of information technology, including security and data protection.

Security Program 1.0 - Michigan at the time of this consolidation protected its infrastructure using the classic demilitarized zone (DMZ) approach to security. While this approach was adequate in the 1990's when the state had few e-government services, security planners in the newly created Office of Enterprise Security (OES) recognized that the state's risk was rapidly increasing as the number of e-government applications increased and the nature of the Internet threat changed.

The Changing Internet Threat – No longer were Internet threats being caused by computer hobbyists, but rather by a more sophisticated criminal element whose purpose was to perpetrate fraud on individuals and organizations. The increased sophistication and maliciousness of cyber security threats created unique challenges for Michigan.

Defense-in-Depth Strategy - To solve the challenges, OES began its "*Security 2.0: Next Generation Security Program".* The strategy used in developing this program was based on Defense-in-Depth or layered defense. Rather than having a singular point-base security solution, the new program would implement multiple layers of defense to protect state assets. In this manner, if a particular layer is breached, the next layer will catch the breach.

The Plan

Strategic Planning - The initiative began with a Return on Investment (ROI) study to identify effective solutions which could be implemented given Michigan's scarce resources and limited finances. This resulted in a strategic plan which was briefed and approved by the Michigan Information Technology Executive Council (MITEC)[1]. To fund the program's equipment and software, OES applied for and received a number of Homeland Security grants. To fund the day-to-day operations, OES received approval from MITEC to increase its yearly security allocation.

Mitigating the Malware[2] Threat

Enterprise Filtering Systems - OES recognized that the threat profile for both spam e-mail and web surfing was changing. The "bad guys" had started to successfully use both spam e-mail and rogue websites as mechanisms to deliver malware[3] . To counter this threat, OES implemented two enterprise filtering solutions to mitigate the malware risk and to eliminate spam.

The first solution by Trend Micro prevents spam e-mail from being delivered to state employees and removes malware from non-spam e-mail. The second solution by SurfControl prevents state employees from surfing web sites that have been determined to be a risk to the state's infrastructure.

Vulnerability Assessment

Monthly Vulnerability Assessment Program – During its threat analysis, OES identified three alarming trends. First, the number of operating system vulnerabilities being discovered for systems used by the state was rapidly increasing. Secondly, the number of those vulnerabilities which could be exploited

[1] MITEC is made up of Deputy Directors from each Executive Branch agency.

[2] Malware is any program such as a virus, Trojan, or botnet installed on a system to internally cause harm.

[3] The intent behind the malware was to hijacking sensitive information such as credit cards, log-in and passwords

remotely was also sharply increasing. And finally, the number of remote exploits that would give the attacker access was also skyrocketing. To determine how these trends effect Michigan, OES had a third-party perform a network penetration test.

The results of the penetration test led OES to develop another layer to its defensive strategy. In addition to scanning systems as part of its change management process, DIT began to proactively scan all of its public facing devices each month. Vulnerabilities that have been discovered by the scans are then sent to infrastructure and application teams for remediation. To ensure that progress is being made in remediation a monthly score card is generated by OES and delivered to DIT executive management.

Security Readiness and Response

Network Anomaly Detection and Event Correlation - To stop cyber attacks that might penetrate the state's defenses, OES has implemented a network anomaly detection system and an event correlation system. The anomaly detection system gives staff the tools to monitor and detect abnormal network activity occurring in real time across the enterprise. The event correlation system collects logs and lists of actions that occurred from various systems, firewalls, routers, Intrusion Detection Services and other network devices. The correlation tools analyze the logs in real time and provide a dynamic and broad picture of unfolding events. Both systems allow staff to implement counter measures faster to contain the threat before it gets out of hand.

Emergency Coordination Center - To coordinate the activities should a cyber disaster occur, OES developed and implemented an Emergency Coordination Center (ECC) based on the National Incident Management System (NIMS). The center is activated in a time of emergency and interfaces directly with the state's Emergency Operations Center. In 2006, the Michigan ECC was one of three states to participate in the Department of Homeland Security's Cyber Storm exercise, a global exercise of 300+ participants that focused on a national response to a cyber security event.

Security Awareness - One of the best protections against the loss of confidential electronic information is to train computer users in IT security awareness. As part of its program, OES implemented the Michigan IT Security Awareness Web Portal[4] to reach out to citizens, and state employees to provide information related to computer and network security.[5] The site also includes the Michigan Online Security Training (MOST), for state employees. This site has been reviewed by a number of national magazines and referenced by a number of other states.

Local Partnerships - OES as part of its security program has reached out to local units of government and educational institutions in Michigan by creating the Michigan Information and Sharing Analysis Center (MI-ISAC) as a means of raising the level of cyber security readiness and response within the state. The MI-ISAC provides local units of government as well as educational institutions in Michigan with a central resource for gathering and sharing information on cyber threats to critical infrastructure throughout Michigan.

B. Significance to the Improvement of the Operation of Government

The Security 2.0: Next Generation Security Program has and continues to have a significant impact on the availability, integrity, authentication, confidentiality and non-repudiation of Michigan infrastructure. And thus has provided the foundation for a successful implement of Michigan's e-government program. The following are benefits that have been realized as part of the program.

[4] http://www.michigan.gov/cybersecurity

[5] Security issues such as : Computer virus threats, protection of confidential and sensitive information, Internet and email usage, physical security, wireless risks, recommendations for avoiding fraud and identity theft, and other best practice security information.

Benefits of Filtering Programs

The effect of spam, viruses, and e-mail attacks on a state's business functions can be significant. The spam filtering solutions implemented by OES last year (2006) blocked 9.1 million e-mail messages or 81 % of the total messages received by the state. They blocked 547,000 malware infected e-mails. In addition, the Internet filtering system blocked 1,675,492 connections to spyware related websites. These numbers translate into the following benefits in state operations:

- *Improved processing time* – The amount of time necessary to process messages through switches, routers and servers has been decrease by reducing the e-mail workload.
- *Improved bandwidth usage* – Bandwidth is a finite resource. Reducing the number of e-mails being delivered across the network and reducing the number of infections increases the amount of bandwidth available to do state business.
- *Better management of IT resources* – Reducing the number of PC infections has reduced the number of visits made by IT techs to out-state sites. Reduced visits equates to reduced staff. This reduces the IT costs for end users and results in the better utilization of existing staff.
- *Reduced hardware and software costs* – The state has been able to reduce the number of servers, amount of disk storage and the number of software licenses needed to deliver e-mail. In addition, in the case of SurfControl, we were able to consolidate resources thus saving hardware and software.
- *Less downtime* – by having proactive monitoring and filtering of Internet threats we have less infections. Fewer infections equate to less down time for the state worker who cannot work because of an infection.
- *Better End-User Experience* – State workers have a better end-user experience by having less e-mail to wade through, by having better response time, and by having less downtime of PC and systems.

Benefits of Vulnerability Assessment

Security is all about risk reduction. The monthly vulnerability assessment program implemented by OES has had a positive impact on state operations by reducing the threats and preventing intrusions. During it's year in operation this program has reduced the number of vulnerabilities found in state systems by 412%[6]. This translates into the following benefits for state operations:

- Lowers the cost of operating systems by improving security posture and reducing exposure to high-risk vulnerabilities.
- Improves productivity and operational efficiencies by reducing system and application downtime.
- Provides uniform management of vulnerabilities across enterprise applications.
- Reduces the total cost of ownership by centralizing network vulnerability monitoring.
- Allows state to meet Payment Card Industry compliancy guidelines.
- Improves the productivity of system administrators who are responsible for vulnerability remediation

Benefits of Security Readiness and Response

The establishment of the ECC and the processes and procedures that support its operation has a positive effect on state employee productivity by shorting the amount of time a piece of infrastructure is down as a result of an emergency, be it a virus outbreak or a power outage.

[6] Fourth Quarter 2005: 318 Vulnerabilities, April 2007: 77 Vulnerabilities

Reputation

As Othello said "Reputation, reputation, reputation – the one immortal part of man." These programs have played and important role in keeping Michigan's Internet services safe and available. And in doing so have made these services available when needed by the citizens of Michigan.

C. Public Value

1. Benefits realized by service recipients, taxpayers, agency or state

Improved Availability of E-Government and Critical Services

The filtering, vulnerability assessment, Network Anomaly Detection and Event Correlation programs all keep infrastructure availability consistent by either mitigating the risk of installing malicious code, patching vulnerabilities or detecting risks as they are getting started. Increased availability means that a prospective new business owner can get an on-line permit, a taxpayer can inquire on the status of their tax return or download the current form or a local police officer can pull the wants and warrants on a subject that has just been pulled over.

Better Business process integrity

The citizens of Michigan rely on state government to protect the confidentiality of information that it has as a result of their interaction with the state. In fact, this year the Rossman group, a Michigan based public relations firm, found that Michigan residents feared the loss of personnel information, identity theft, more than they feared the loss of a job, a home foreclosure or a terrorist attack. Each of the technology based programs reduce the risk of security breaches which could lead to the release of citizen's identity information.

Improved Cyber Security Awareness

All Michigan citizens benefited from the launch of the state's cyber security web portal. The portal gives citizens, students, business leaders, and employees a place to research security issues such as : computer virus threats, protection of confidential and sensitive information, Internet and email usage, physical security, wireless risks, recommendations for avoiding fraud and identity theft, and other best practice security information. The better informed these individuals are the less likely personnel and state assets will be compromised.

The establishment of the MI-ISAC provides local units of government, many of whom do not have the staff to keep current of cyber security issues, with a place to get and share information. Their interaction with state and federal officials translates to better infrastructure support for their local citizens.

Improved Communications during a disaster

The establishment of the DIT Emergency Control Center and the establishment of processes and procedures to use during the time of an emergency benefit citizens both directly and indirectly. For example, in February 2006, Michigan demonstrated the benefits by participating in a global exercise named Cyber Storm. The Michigan ECC, using the integrated tools, procedures and organization developed and implemented via these projects was able to demonstrate its ability to quickly recover from a massive global cyber attack.

2. Return on investment, short-term/long-term payback

Although security ROI can sometimes be difficult to identify, the following calculations exhibit specific benefits for both the short- and long-term payback to Michigan taxpayers.

$403,200 in Annual Savings of the Internet Spyware Filtering Solution

In 2006, there were 1,676,492 blocked connection attempts. In reviewing the workstation destination information on these blocks, we found that 4,600 workstation would have been infected if the connections were not blocked. In addition, we found by monitoring trouble tickets that on the average we had 120 machines infected after the new solution was implemented. So the total annual cost avoidance for this

solution is calculated by subtracting the Total Infected Cost after SurfControl (TICAS) from the Total Infection Cost without SurfControl (TICWOS)

TICAS = 4,600 infected machines/month * 3 hrs/repair time * $30/hr repair cost or $414,000

TICWOS= 120 infected machines/month * 3 hrs/repair time * $30/hr repair cost or $10,800

ROI = $414,000-$10,800 or $403,200

$3,796,745 in Annual Savings of the Spam Filtering Solution

Annual savings is determined by estimating the total labor cost saved by elimination of spam from a users e-mail. The assumption is that it takes 5 seconds for a user to process a spam e-mail. The calculation is as follows:

ROI = 7,593,490 e-mails/month * 5 sec/e-mail * 1 hr / 3600 sec * $30/hr * 12 months/year
ROI =$3,796,745.

$437,250 in Annual Saving in the Time to Perform Investigations

The tools implemented as part of the Vulnerability Assement program reduced the amount of time it takes to complete a forensic investigation from 50 hours to 17 hours per incident. The difference between the two numbers represents the annual savings.

Before Implementation Costs = 265 incidents * 50 hours / incident * $50 /hr labor = $622,500
After Implementation Costs = 265 incidents *17 hours / incident * $50 / hr labor = $225,250
ROI = $622,500 - $225,250 = $437,250

$6,069,347 in Annual Savings by Reducing Breaches

Internet Security Systems[7] gathered data on Michigan's potential IT losses during a ROSI workshop and determined that the state could expect to reduce its annual loss from confidentiality, integrity, and data availability (CIA) breaches through the implementation of the critical IT protection solutions identified in the strategic plan. The following long-term paybacks could be realized:

- Confidentiality breach - Reduce potential annual tangible costs from $1,927,800 to $1,272,348, shows savings of $655,452
- Integrity breach- Reduce potential annual tangible costs from $1,624,350 to $1,072,071, shows savings of $552,279
- Availability breach - Reduce potential annual tangible costs from $14,298,870 to $9,437,254, shows savings of $4,861,616

Annual CIA savings = $655,452 + 552,279 + $4,861,616 = $6,069,347

Total Annual Return on Investment of $10,706,542

Based on the cost savings from Internet spyware filtering, anti-spam filtering, investigation savings, and potential CIA breach prevention, the Security 2.0: Next Generation Security Program is producing a conservative cost savings of:

Internet Spyware Filtering	*$403,200*
Spam Filtering	*$3,796,745*
Total Annual Investigations Savings	*$437,250*
Annual CIA savings	$6,069,347
Total Annual Return on investment	*$10,706,542*

[7] The company provides security products and services that preemptively protect enterprise organizations against Internet threats. It was recently purchased by IBM.