

NASCIO 2006 RECOGNITION AWARDS NOMINATION

Title of Nomination: Critical Infrastructure Resiliency and Continuity Project

Project/System Manager: Dan Lohrmann

Job Title: 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

Category: Business Continuity Category

Person nominating: same as above



Office Of Enterprise Security

DEPARTMENT OF INFORMATION TECHNOLOGY

Critical Infrastructure Resiliency and Continuity Project: Executive Summary

In “Taking Control of IT Risk” (Michael Rasmussen 2/2006) Forrester makes a point that an organization needs to take a holistic approach to dealing with IT risk. That an organization’s ability to continue profitable operations within IT critical information systems is dependent not only on its ability to address risk caused by major events (e.g. hurricanes, tornados and power outages) but also being able to mitigate and recover from risks caused by daily exposure to malicious attacks from terrorists, hackers, worms, viruses and the inappropriate control of sensitive and regulated information. In implementing the Critical Infrastructure Resiliency and Continuity Project (CIRCP) the Michigan Department of Information Technology (MDIT) estimated it saved the State of Michigan approximately \$31,000,000 and kept critical systems and processes operating when others were not as fortunate (e.g. Zoto worm 8/2005). MDIT believes that other organizations can benefit in reviewing this project and the lessons learned.

In developing the Critical Infrastructure Resiliency and Continuity Project, MDIT used best practice methodologies that included prevention through technology and training; mitigation of cyber breaches through new technologies and supporting organizational structures; and improved response processes and technologies to address cyber incidents and emergency situations when they occurred. MDIT undertook a Return on Security Investment (ROSI) analysis, recognizing the principle that ignoring constant daily exposures could be as detrimental to the continuity of the state IT infrastructure as a catastrophic event. The ROSI study identified six solutions that could be used to prevent, mitigate, respond and recover from incidents involving terrorism or other cyber attacks. The ROSI analysis also persuaded MDIT’s state agency customers to double the security allocation from 1% of the IT budget to 2%. MDIT verified the project’s effectiveness by recovering from global cyber attacks as part of the Department of Homeland Security Cyberstorm exercise.

The solutions identified by MDIT were:

The Authentication and Access Control Technologies solution included Internet access control filtering for risky websites; email anti-virus and anti-spam filtering to increase data availability and employee productivity; and a digital video manager system used at critical IT datacenters to deter and respond to physical attacks.

The Cyber Vulnerability Assessment Program solution included network scanning, intrusion detection systems, and network penetration study and assessment. This project identified exploitable entryways into the SOM networks.

The IT Security Awareness Web Portal solution hosts a website providing best practice IT security information for computer users throughout Michigan. The website also seeks to bolster security for Michigan’s businesses and in turn bring new jobs and economic development to Michigan.

The Event Correlation solution accumulates data from various security systems and looks for significant patterns that indicate cyber attacks or intrusions.

The Forensic Incident Investigation solution includes recovery devices that examine and preserve digital evidence in a forensically sound manner and response information distribution devices to distribute the evidence of a cyber-related incident to appropriate law enforcement agencies.

Install generators for mission critical datacenters to allow for continuity during power outages.

A. Description of Project

As a result of an explosion of cyber crime and daily cyber attacks against the State of Michigan (SOM), the Michigan Department of Information Technology (MDIT) undertook a Return on Security Investment (ROSI). The purpose of the ROSI was to determine which solutions, given the state's scarce resources and limited finances, would be the most effective in preventing, mitigating and responding to these attacks. A strategic plan for the mitigation of cyber attacks was developed and briefed to the Michigan Information Technology Executive Council (MITEC), made up of Deputy Directors from each Executive Branch agency. MITEC agreed with the strategy and voted to approve the plan. In addition, MITEC voted to double the security allocation from 1% of the IT budget to 2%.

Six major solutions were identified and implemented by MDIT and exhibit MDIT's accomplishments: The Authentication and Access Control Technologies, Cyber Vulnerability Assessment Program, IT Security Awareness Web Portal, Threat Events Correlation System, the Forensic Incident Investigation Systems, and new generators.

Solutions within the Authentication and Access Control Technologies consist of:

- The Internet Access Control and Filtering project used SurfControl technology to filter Internet access for all state executive branch agencies. This solution prevents cyber attacks against critical SOM IT systems by blocking access to websites that are deemed risks to the state's critical infrastructure. Filtering Internet access reduces the risk of disclosure of confidential information or the disruption of government operations. This project was implemented enterprise-wide in January 2005 and has demonstrated significant benefits in reducing bandwidth usage, preventing viruses, Trojan programs, spyware, phishing scams (i.e. when a person is tricked into divulging sensitive information), and other damaging effects to critical IT infrastructure.
- The Email Anti-virus and Anti-spam Filtering solution used Trend Micro products to upgrade the anti-virus protections and block spam emails for all SOM email users. Implemented November 2004, this solution prevents email virus and worm infections, email scams that trick employees into divulging confidential information, and allows employees to focus on business-related tasks.
- Physical security at the IT datacenters has been improved through a Digital Video Manager (DVM) system comprised of digital video cameras and a primary and backup system for viewing, archival, and retrieval that includes disaster recovery capability. Implementation of the DVM began in January 2005 and has ensured improved access control and surveillance of critical IT infrastructure to protect against physical attacks to these sites.

The Cyber Vulnerability Assessment Program solution includes network scanning, intrusion detection systems (IDS), and network penetration study and assessment. This project identified specific and exploitable vulnerabilities within the SOM networks and exposed potential entryways into vital and sensitive data. Third-party network intrusion experts mounted an attack from the Internet using a minimal amount of information that would be publicly known about the SOM networks. If they were able to penetrate the systems, the average cyber attacker would also be able to obtain access to the systems. Vulnerabilities that were discovered were reported for remediation allowing the SOM to preempt any cyber intruder by patching the weaknesses before a real exploit occurred.

The IT Security Awareness Web Portal solution hosts a website (<http://www.michigan.gov/cybersecurity>) providing IT security information for computer users throughout Michigan. Launched in April 2005, this website reaches out to all citizens of Michigan, state employees, and home

computer users everywhere and has received extensive national press coverage. The project's purpose was to provide a better understanding of security issues that include: 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. One of the best protections against loss of confidential electronic information is to train computer users in IT security awareness. The website includes MOST, Michigan Online Security Training, for SOM employees. After reviewing the information, the user is asked to take an online quiz to measure knowledge obtained from the training. A high enough score allows the employee to print off a certificate of accomplishment.

The Threat Events Correlation System accumulates data from various security systems (e.g. IDS, firewalls, inbound Internet email gateway, and all SOM desktop anti-virus systems) and looks for significant patterns that indicate cyber attacks or intrusions. Any computer virus infection that is detected at the computer user's desktop reports this event to the incident management coordinator through the event correlation collector. Correlation of events provides a broader picture of unfolding events and allows prevention of wide-spread computer virus outbreaks as well as a more timely response to a cyber attack.

The Forensic Incident Investigation solution includes:

- FRED devices (Forensic Recovery of Evidence Device) preserve and examine information in a forensically sound manner in order to respond and recover from a cyber-related incident against the SOM's critical IT infrastructure. This project allows data to be gathered without compromising or contaminating the evidence for potential investigation and criminal prosecution.
- The Rimage system is used to distribute, via DVD, response information (e.g. video surveillance) and evidence of a cyber-related incident against the SOM's critical IT infrastructure. This system allows collaboration with other first responders and law enforcement entities and is used to preserve digital evidence for investigation and criminal prosecution.

Two new generators were installed in December 2005 at critical state data centers.

Mission critical systems were found to be at risk during the power outage of August 2003, so this project was given a high priority to ensure the continuity of Michigan government.

B. Significance to the Improvement of the Operation of Government

The solution projects described above have demonstrated significant and measurable benefits for the operations of SOM government and the citizens of Michigan as shown through the following six examples:

1.) The Internet Access Control and Filtering solution using SurfControl technology blocks access to websites that are not business-related which improves the operation of government. This prevents the employee from being tempted into surfing the Internet instead of focusing on government business. In addition, blocking access to websites that utilize excessive bandwidth (e.g. advertisements and popups) improves the operation of government by increasing connection time to the Internet for business-related work and lowering connection costs.

2.) The Cyber Vulnerability Assessment Program has improved operations of government through prevention of cyber exploits and compromise of confidential citizen information by identifying vulnerabilities within the network from the network scanning and penetration study assessment.

Exposing backdoors into the network and systems provided opportunities to correct the entryways, remediate the vulnerabilities, and establish a more secure network.

3.) An example of a cyber incident that occurred in early 2005 demonstrates how several of the critical IT protection solutions mitigated a cyber attack and improved operations of government. Using tools acquired under the Cyber Vulnerability Assessment Program, network analysts monitoring the IDS in real-time and noted that Internet Relay Chat (IRC) was being exploited on state computers. The systems were compromised and the attacker took remote control of the computers.

The IDS was used to identify open ports that should not have been available. The SurfControl logs (from the Authentication and Access Control solution) were analyzed and it was found that the compromised computers were communicating with a computer in Brazil. Using the SurfControl real-time monitor, it was shown that connections were occurring every 15 seconds or less. As no human could do this manually, it was determined that this had to be an automated connection. The SurfControl Top Ten Report function was utilized to verify the data for connections made. The compromised computers were immediately removed from the state's network. Next, the FREDs (from the Forensic Incident Investigation solution) were used to image (make a copy of) the compromised computers' hard drives. The forensic software was then used to analyze the data. It was determined that the compromised computers had been sending data to the hacker for more than a month. Fortunately, the mitigation and response actions taken prevented any critical or confidential data from being sent to the attacker.

The final step used the Rimage system to archive the computer images and evidence. Multiple DVDs were then distributed to law enforcement, including the Michigan Computer Crime Unit for review, investigation, and possible prosecution. A report was written using forensically sound evidence and sent to the US-CERT (United States Computer Emergency Readiness Team).

4.) In December 2004, there was a 4-fold increase over 2003 in the amount of email virus traffic blocked at the SOM's Internet gateway. Implementation of the upgraded anti-virus solution (from the Authentication and Access Control solution) improved operation of government by preventing cyber exploits from computer viruses and other malware sent through email.

5.) The Event Correlation project was implemented in April 2005. During this time the SOM has seen benefits to the operation of government. The event correlation technologies determined that all state computer clients (e.g. desktops, laptops, etc.) had not been uniformly configured to prevent virus infections. The state is in the process of working to correct these configuration errors through the anti-virus parent server structure by forcing the correct configurations down to the desktop. This ensures that all computers have the most effective anti-virus protection. In addition, the Event Correlation project has identified significant virus and spyware incidents that had not been previously visible or reported at the enterprise-level. The importance of having one place to collect threat information has allowed the SOM to develop metrics identifying vulnerable areas requiring attention.

6.) One of these new generators provided backup power during a complex-wide power outage which was experienced in February 2006. This unscheduled electric utility outage sent thousands of state employees home. As a result of the new generator, critical servers stayed operational during the eight hour outage, which enabled government services to keep running state-wide. These new generators have enabled the state to provide essential services to state agencies and centralize many servers into these more secure and redundant facilities.

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

Five key benefits realized by citizens, the SOM, and its business partners are explained next.

1.) In February 2006, the SOM demonstrated the benefits of the CIRCP by participating in a global exercise named Cyber Storm. The Department of Homeland Security designed this exercise to test, evaluate, and improve communication, coordination, and procedures between government and private sectors organizations worldwide. The SOM 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.) Spyware can be loaded onto a computer without the computer user's knowledge to steal sensitive information like passwords and credit card numbers and poses a real risk for identity theft to citizens. The Internet Access Control and Filtering solution using SurfControl technology blocks all state employee's access to spyware websites. This provides direct benefits to Michigan citizens and state government by preventing the exposure of confidential information.

3.) In 2005, over 53% of all reported fraud complaints to the Federal Trade Commission (FTC) were Internet-related. Citizen, state, and agency confidential information has been protected through the blocking of websites that attempt to trick the computer user into providing information that is confidential. The criminals try to exploit the victim by selling the confidential information for financial gain or using it to commit identity theft. These websites often automatically download to the computer harmful Trojan programs or viruses by just clicking on the link when the website is visited. Other harmful website categories that are blocked are: Adult/Sexually Explicit, Advertisements & PopUps, Chat, Gambling, Intolerance & Hate, Personals & Dating, Violence, Games, Remote Proxies and Peer-to-Peer.

4.) In December 2004, two weeks after implementation of the anti-spam solution, the state saw more than 740,000 spam emails blocked. Blocking spam-related emails allows more time for state workers to do business-related tasks and also protects the computer user from receiving the phishing emails that try to trick them into clicking on a link to the spyware or virus-laden website.

5.) All Michigan citizens benefited from the launch of the state's cyber security web portal. Besides educating citizens on best practices for IT security, the website seeks to bolster security for Michigan's businesses. Because a presence on the web is so vital for any business in today's technologically driven economy, websites and electronic transactions must be secure. The cyber security portal educates leaders on business continuity, personal privacy and the physical security of IT assets. By creating secure technological environments, businesses can develop strong, healthy infrastructures and in turn bring new jobs and economic development to Michigan.

D. 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.

SurfControl metrics show that approximately 800,000 blocked connection attempts to spyware websites occur every month (note: one machine can be infected with multiple spyware infections which translates to approximately 8400 machines). Every machine that has been infected with spyware must be physically visited to clean and restore functionality to the computer. With SurfControl protections, the SOM currently averages 180 spyware infections per month that require cleaning. At \$30 per hour (Field Technician wages and benefits) X 3 hours (average repair time) X 180 (monthly machine infections) = \$16,200 in cost for spyware repairs per month. Without SurfControl's spyware blocking the potential cost would be approximately \$30 X 3 hours X 8400 possible machine infections = \$756,000. SurfControl's spyware block shows a cost savings of \$739,800 per month.

Annual Internet spyware filtering savings = \$8,877,600

SurfControl metrics show that bandwidth usage was reduced by 37% between January – May 2005. This is primarily due to the Popup and Advertisement category block.

After Internet emails are filtered through the anti-virus gateway, the SOM is left with approximately 4,800,000 emails per month. About 54% of these are spam emails. Average monthly spam emails blocked at the Internet gateway total 2,608,000. The anti-spam implementation at the gateway shows a return on investment in number of blocked spam emails that would have taken time away from business-related efforts. If 1 minute is spent reviewing a spam email (one that is not even malicious), the time saved in blocking the spam emails per month = 43,467 hours. Annual hours saved = 521,604 X \$30 hour (wage and benefits):

Annual anti-spam savings = \$15,648,120

Prior to the Cyber Vulnerability Assessment Program, the Forensic Incident Investigation solutions, and the SurfControl implementation, a computer incident investigation would take between 40-60 hours to complete. A calculation of 50 hours X \$50 (specialist wage and benefits per hour) X 103 incidents (based on 2004 statistics) = \$257,500 annual incident investigation cost. With the new technologies implemented from the critical IT protection solutions, incident investigations have been reduced to 15 – 20 hours. This calculation shows 17 hours X \$50 hour X 103 incidents = \$87,550.

Annual investigation savings = \$169,950

Internet Security Systems gathered data on the SOM's largest potential IT losses during the ROSI workshops. Based on these statistics, it was determined that reducing expected annual loss from confidentiality, integrity, and data availability (CIA) breaches through the critical IT protection solutions, 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 = \$6,069,347

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

Total Annual Return on Investment = \$30,765,017

In conclusion, the solutions of Authentication and Access Control Technologies, Cyber Vulnerability Assessment Program, IT Security Awareness Web Portal, Threat Events Correlation System, Forensic Incident Investigation System, and the new datacenter generators will continue to provide long-term return on investment and business continuity as the SOM government moves forward with the business of serving the citizens of Michigan.