Cybersecurity & Infrastructure Protection
State of Michigan
Department of
Technology, Management & Budget

2013 NASCIO RECOGNITION AWARD NOMINATION

Cyber Training 3.0: New Solutions Addressing Escalating Security Risks

Nomination Category: Cyber Security Initiatives

Name of State Agency:
State of Michigan
Department of Technology, Management & Budget (DTMB)

Project Manager:
Dan Lohrmann, Chief Security Officer
(517) 241-4090
Lohrmannd@michigan.gov

Name of Project Executive Sponsors:
David Behen, State CIO
John Nixon, Director DTMB and State Budget Director
Michigan Governor Rick Snyder

Project Initiated: July 2011
Project Completed: November 2012

2012 Breakfast Conference Series

Michigan Cyber Range Facility Opening November 2012

Statewide Cyber Awareness Training Implemented September 2012

Section 2 - Executive Summary: New cyberattacks, mobile malware, insider threats and unprecedented security challenges threaten to derail innovative government strategies. At the same time, human error plays a role in 63% of IT security breaches. After previous efforts failed to change actions, new training approaches were deemed essential for government end users and technical staff. In response, Michigan launched a comprehensive three-pronged approach that holistically addresses employee awareness, technical training and cultural change components for businesses, schools and families. This integrated program addresses the significant training needs to secure information by addressing our greatest asset and also our greatest risk – our people. This program is easily transferable to other government entities nationwide.

Problem Statement: In response to an unprecedented increase in cybersecurity threats, significant training needs, audit findings and public awareness needs on cyber-safety, a comprehensive overhaul of end user cyber awareness training and technical cybersecurity training was required to address cyber risk reduction. The average cost of a breach in 2011 [1] was $5.5 million per organization. Meanwhile, early attempts to provide end user and technical training were viewed poorly by staff, with comments like "boring" and "irrelevant." Training for technical staff was not keeping pace.

Solution: Michigan selected *Security Mentor* to offer a new cyber awareness training program to all state employees for about 30 cents per lesson for over 50,000 state and local employees. Twelve 10-minute self-paced training modules are offered online as a service via the Internet from the vendor's facility. This interactive, refreshed awareness solution covers the top cyber risks facing government. Also, our Cyber Breakfast Conference Series spread the word state-wide in 2012 with expert presentations, and our 2011 Cyber Summit was the national kickoff for Cybersecurity Awareness Month.

The new Michigan Cyber Range offers a research, test, training & evaluation facility for cybersecurity and cyberdefense, addressing the needs of our technical workforce. In partnership with universities, the private sector and governments, Merit Network Inc, a 501c3 nonprofit organization, was chosen to build and develop this state-of-the-art center to further advance cybersecurity training across Michigan and the USA.

Significance: Our training efforts have reduced the potential of a data breach by continually training end users and spreading the word to every part of Michigan. We are changing enterprise culture to be more security-aware. One example is a special project that resulted in over a thousand messages per month now being sent from end users to our mailbox for suspected scams and spear-phishing attacks. Also, the Michigan Cyber Range has become a national center for training cybersecurity staff, with numerous state and local governments, companies and educational institutions expressing interest in receiving training at our cyber range training cybersecurity staff.

Benefits: The program has achieved significant improvements in governance, procedures, operations and risk management outcomes:

- Closed 11 audit findings, new training approaches over 50K employees.
- Improved regulatory compliance (such as PCI) through covering security gaps.
- Reduced breach potential and improved security response and communication.
- Training capability & partnerships enhanced with local and national organizations.
- Video training on cybersecurity and citizen and business online safety are available at Michigan.gov covering National Kickoff Cyber Summit, Cyber Road Shows, and the Cyber Breakfast Conference Series. Increased public and government awareness resulted from these efforts.

[1] 2011 Cost of Data Breach Study: Ponemon Institute, LLC (March 2012)

Section 3 - **Business Problem:** As the number of data breaches in the public and private sector has skyrocketed over the past several years, two statistical facts stand out as clarion calls to state government executives to completely realign their cyber training programs. First, the majority of data breaches occur as a result of end user actions. The top preventative measure taken following a breach was the implementation of an effective user training and awareness program (53%). Second, the unemployment rate regarding cybersecurity professionals is zero.

As demonstrated by the frequency of staff clicking on malware-infected links and poorly selected passwords for mission-critical applications, new cyber awareness approaches were vital. The SANS Institute declared that over 95% of recent breaches originated with spear-phishing messages. Internal surveys revealed that our employees felt our training was old, boring, "death by PowerPoint" and not worth completing. A comprehensive new approach to employee training was needed to change culture.

In addition, new partnerships were needed reaching across public/private sectors as well as federal/state/local governments and education groups for technical training of IT staff. Cyberattacks in Michigan could have dire economic consequences for the region and the nation. Developing world-class cyber-defenders will not only help Michigan, it will also help the nation continue to thrive in an age of increasing cyber-threats. Michigan already has many of the nation's top higher education cybersecurity programs and a growing cybersecurity industry.

US Representative Mike Rogers recently highlighted the many serious national cyber threats facing the nation and families. He added that "…About 80 percent of the cyber security problems can be solved with regular computer hygiene — strong password, firewall and virus protections that citizens need to exercise diligently…." Effective awareness and training is job #1 in addressing our cybersecurity challenges.

Solution Description: The state developed a comprehensive cybersecurity strategy which addressed threats in 2011, and our new three-pronged approach to changing culture was an essential element to our risk reduction approach. By grouping innovative awareness training, technical training capabilities and public awareness cyber summits and roadshows together, the cumulative effect of this program is strengthened and impact is greater.

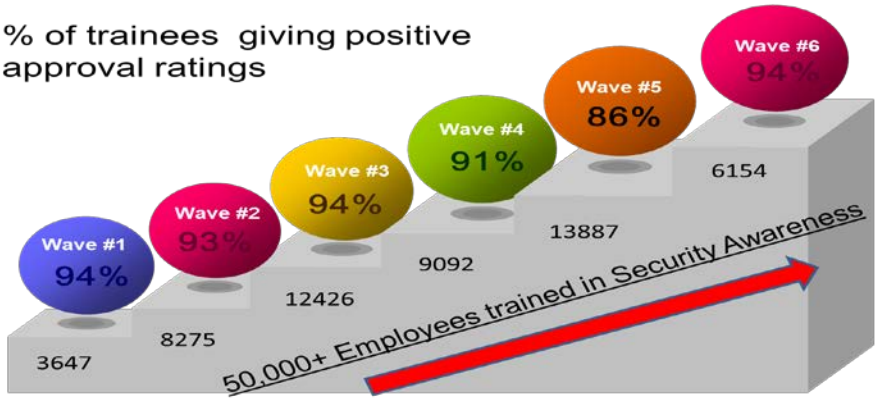
To address growing cyber threats facing federal, state and local governments, businesses, citizens and schools, Michigan has partnered with nationwide organizations to reinvent our education for cybersecurity. Cyber Training 3.0 implements solutions that include effective cybersecurity awareness training for all state employees, cyber toolkits for citizens, schools and small businesses, cyber awareness breakfasts, cyber summits every two years and in-depth technical training for security professionals.

Part 1: ***Awareness Training*** – Michigan has thrown away the old, boring, ineffective cyber awareness training for end users and implemented a new cutting-edge education and awareness training that reduces risk – and that staff and partners have praised. Comprehensive, effective end user awareness training and education is recognized as the single most effective component in the prevention of data loss or a security breach.

After extensive work with customers regarding requirements, we issued a Request for Proposal (RFP) which offered "Next-generation awareness training offering intriguing content which is engaging, interactive, relevant, timely and shown to reduce risk." The contract was awarded to Security Mentor for offering commercial-off-the-shelf, web-enabled training that is self-paced and shown to be effective (with metrics) and reporting

tools. Customer's feedback on training was very positive with quotes like: "Short/Simple/Perfect," "This was awesome!!" "Very thought provoking." "Thank you…"

Twelve 10-minute self-paced training modules are offered online as a service via the Internet from the vendor's facility. The training has been rolled out in six waves to over 50,000 employees and contract staff. Other units of government (such as the legislature, courts and counties) are using our training voluntarily. The chart below indicates total training following each "wave" release (county employees are not included).



Cumulative Total of Employees Trained

Part 2: ***Michigan Cyber Range*** – Michigan built a flexible cyber security range and program to meet the twenty-first century needs of critical infrastructure defense, homeland security, criminal justice and education. Cybersecurity differs from other technical disciplines in that it involves a thinking, adaptive adversary. The best way to improve defensive capabilities in this area is to practice against those adversaries. To meet this need, we chose Merit Network Inc. to begin operating a cybersecurity range and program. The project is a public-private collaboration that includes government, the National Guard, universities, community colleges, K-12 schools and private industry.

The Michigan Cyber Range is a program that leverages the physical range to develop world-class, cybersecurity professionals. There is a full program of meetings and workshops, as well as tools to develop and promulgate best practices in cybersecurity training and cyber security itself. The Range is used for individual as well as collective training. The staff are experts in the best practices of cybersecurity training, meeting the specific needs of the people and organizations that use the Range.

The Michigan Cyber Range is an isolated system that runs on top of Merit's research and education network. It is comprised of sites and racks. Multiple sites contain a number of Range Racks (based on Global Environment for Network Innovations (GENI) racks) and Management Racks. Each Range Rack can support up to 1,000 nodes and 1,000 connections. Sites are located on Merit's network and are connected by layer 2 channels for safe control and operation. Nodes are principally virtualized, and can be any device that connects to a network such as servers, routers, firewalls, etc. The Range can also include other non-virtualized hardware so that it can encompass a wider variety of systems. The traffic will be synthetic, replayed or mirrored. The Michigan Cyber Range is fully capable of recreating portions of the Internet so that cyber security training can be realistic, effective and safe.

A wide variety of courses are currently available, such as those shown in this chart.

Michigan Cyber Range Training Modules	
CCNA	Cisco Certified Network Associate Security
CDRE	Certified Disaster Recovery Engineer
CIHE	Certified Incident Handling Engineer
CISSO	Certified Information Security Systems Officer
CNFE	Certified Network Forensics Examiner
CPTE	Certified Penetration Testing Engineer
CVA	Certified Vulnerability Assessor
IS20	IS20 Security Control
ISCAP	Information Systems Certification and Accreditation Professional

The physical range itself is only part of the solution. To be effective, the Range must be maintained and properly configured to meet the training needs of users by skilled staff. Even more important, the Range staff must know security and how to leverage the Range to maximize the benefit to the users. The Range leverages the prior planning, experience and skill development at Merit. The Range staff works with educators, federal agencies and private companies around Michigan and the nation to make the Range a world-class operation. Dozens of staff have been trained already.

Part 3: *Cyber Summits, Cybersecurity Road Shows in Agencies & Cyber Breakfast Series* - Following the sold-out 2011 Michigan Cyber Summit, the cybersecurity team decided to "take the cyber show on the road" and offer the Michigan Cyber Breakfast Conference Series around the state.

These breakfasts were sponsored by private sector funds and offered excellent networking opportunities and up-to-date information on cyber threats and what to do about them to businesses, schools, citizens and governments. A public / private perspective was also offered. Also, cybersecurity roadshows were offered to each Michigan government agency director which explained the current state of risk and recommended actions to take specific to their organization. A 2013 Cyber Summit is being planned in conjunction with the National Governor's Association Center for Best Practices in Cybersecurity.

Section 4 – Significance to Improving Government Operations: This project has immense significance to operations and addresses numerous executive priorities, including CIO risk reduction efforts and people issues. Specifically:

Part I Impact – Significant Awareness Training and Culture Change – The overall training effort and specific Security Mentor Awareness Training offered:

- Effective, new training for ~50K state employees
- Excellent results and feedback from customer groups – with over 90% positive comments and words like: "fun," "excellent," "I will use this at home" and "best ever."
- Training in all core categories that introduce risks, such as passwords, clicking on links, mobile security, web and application security, and others.
- An ongoing program that closed eleven audit findings.
- Comprehensive measurements on employee training.
- New focus on risk reduction with a formal risk methodology approach

Part II Impact –Michigan Cyber Range –

The range and associated center of excellence can be used by a wide variety of organizations for the accomplishment of a complete spectrum of learning objectives. The major components of the Range are nodes, connections and traffic. Each node is a

functioning system, just as it is on the Internet. Examples include routers, switches, web servers, DNS servers, and personal computers. Since these nodes are operating with the actual software that is run in real systems, they have the actual vulnerabilities that are found on the Internet. The connections function the same as the connections in the Internet, within enterprises and inside data centers. Hence configurations ranging from extremely complex to relatively simple can be set up in the Range. The traffic can be simulated to mimic any type of environment; it can be stored and replayed to create the ideal learning environment and it can be mirrored from actual traffic streams. In the latter case, this realism will be unmatched in any other environment and will develop capabilities of the highest level. The Range will be unprecedented in its flexibility, scalability and capability.

As valuable as the Michigan Cyber Range is, the associated center of excellence will exponentially increase the value of the Range to the nation. A cyber range itself is complicated to manage and labor intensive to maintain. Its purpose is to host software that damages the nodes on the network. That damage must be quickly repaired between uses. To serve a wide variety of needs, the Range will have a large library of systems that will be set up prior to use. The ability to quickly and efficiently set and reset the Cyber Range to meet the needs of users will be a critical capability of the Range team.

- Met Governor's mandate, federal requirements and state government requirements to incorporate and modernize training and awareness were satisfied.
- Aligned with Federal, State, CIO and NASCIO priorities in cybersecurity.
- Created new opportunities to provide critical cybersecurity certifications to technical staff and close the gap with those attacking us.

Operations:

- Creation of a new public/private Michigan center of excellence staffed and utilized by people who are not only experts in security, but experts in teaching users and trainers how to succeed in cybersecurity.
- Metrics for operational improvements and required cyber actions to reduce risk.
- A common security "road show" for agencies to understand and act on cyber risk.
- Establish a national best practice that numerous other states are using.

Part III - Specific Significant Full Scope Efforts: Greatly improved cyber awareness campaign that is interactive, relevant and intriguing.

- National launch of Cybersecurity Awareness month at sold-out Michigan Cyber Summit 2011 – see: http://events.esd.org/MichiganCyberSummit2011.aspx
- New cyber awareness toolkit – see: www.Michigan.gov/cybersecurity
- Address nexus between physical security and cyber operations threat activities.
- Set the stage for hosting further events with a national / regional focus – in partnership with organizations like: DHS, MS-ISAC, US-CERT, DoE, and DoD.

Section 5 - Benefit of the Project: *Cyber Training 3.0* has established Michigan as a global government leader in cybersecurity training in less than eighteen months. Benefits are being realized by families, students, government employees, K-20 education, businesses and other states and local governments who have adopted this program. The program has achieved significant improvements in governance (see A,B,K&L), operations (see C,E,F,G), procedures (see H,I,J) and risk management outcomes and procedures (see D&K):

A. These efforts support the Governor's cyber initiatives and NASCIO cybersecurity priorities such as new 24x7 Security Operations Center (SOC), Rapid Cyber Defense Response Team (Public/Private), and a new Michigan Cyber Command Center. (See www.Michigan.gov/cybersecurity for more details.)
B. A coordinated response process and actions for security incidents has been created.
C. The Security Mentor cyber awareness program cost under $200,000 and provides 12 self-paced lessons for all state employees for about 30 cents per lesson over a 2-year period. While hard savings are difficult to show, with an average breach costing over $5 million dollars and the South Carolina breach costing over $25 million, we believe that the ROI for this program is more than 100 to 1. We have stopped numerous breaches from occurring through this program via early identification of malware and spear-phishing scams using newly established procedures and staff training.
D. More than a dozen serious cyber threats have been avoided directly from efforts.
E. The Michigan Cyber Range has been established via grants and private sector donations. Over $2 million was raised to establish the Cyber Range, with less than 20% coming from government sources. State government is saving approximately 40-50% on training as compared to similar courses, and we anticipate a five-year savings of over $500K in certification, course and travel costs.
F. Closed audit finds and streamlined and coordinated training.
G. The Cyber Summits and Breakfast Conference Series were (and will be) self-supporting via sponsorships and fees to attend events. These events have focused media attention on the cybersecurity issues in the Great Lakes and beyond. Videos, training materials, toolkits and more are available at www.Michigan.gov/cybersecurity
H. Strengthened security in existing (and future) infrastructure, cabling, data networks, wireless and mobile computing projects. See: Michigan Cyber Initiative
I. Enhanced existing staffing skillsets in cyber and physical security areas. Also, improved end users training – see: Security Breakfast Roadshow
J. Agency projects completed more securely included: PCI Compliance & IRS audit findings closed (Dept. of Treasury), health information sharing efforts (Dept. of Community Health).
K. Addresses new and emerging cyber threats in constantly 'refreshed' approach.
L. Governor Snyder co-leads the National Governor's Association Center for Best Practices in Cybersecurity. Our efforts have highlighted Michigan's checklist of training options to reduce risk and change culture – including cyber awareness.

In conclusion, this systematic approach to risk reduction offers a transferable approach for other state and local governments to emulate. Our greatest resource, and our greatest risk, is our employees. States need to engage and train customers in new, effective ways. Michigan has taken a look at past training system failures. We've built a new holistic program that enables our government workforce and residents to understand the impact of online actions – and protect their corner of cyberspace.