The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

Status:
Laureate

Year:
2013

Organization Name:
Cybersecurity and Infrastructure Protection (CIP), Michigan Department of Technology Management and Budget (DTMB)

Organization URL:
http://www.michigan.gov/cybersecurity

Project Name:
Integrating Cyber and Physical Security: Ending the Divide Using a Comprehensive Approach to Risk

Please select the category in which you are submitting your entry:
Safety & Security

Please provide an overview of the nominated project. Describe the problem it was intended to solve, the technology or approach used, how it was innovative and any technical or other challenges that had to be overcome for successful implementation and adoption. (In 300 words or less.)

Problem Statement: In response to an unprecedented increase in security threats cyber-attacks, malware, insider threats and other security challenges and in order to maximize overall technology efficiency and effectiveness, the Michigan Department of Technology Management & Budget (DTMB) has ended the divide between the enterprise-wide physical and cyber-security organizations with the establishment of a Cybersecurity and Infrastructure Protection (CIP) function.

Overcoming Cross-boundary Barriers: New partnerships were needed, cutting across public/private sectors as well as federal/state/local governments and various education groups. A cross-sector team assessment team was assembled in April 2011 that included state, local and federal government experts, private sector companies, P-20 education, universities and others. Necessary actions were identifies around three distinct but equally important pillars: confidentiality, integrity and availability. In addition, the need for new governance, risk assessment, defined budget, and an implementation plan starting with access controls was clear. Operational/Technical Solutions: Industry experts advised that as long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one. Principal elements of integrated security included: common access cards, video surveillance, improved emergency management training, joint exercises, situational response, business continuity and data center security. Road Map and Outcomes: This innovative, first in the nation project, along with the implementation of the ongoing training program and development of the Cyber Summit, Cyber Initiative (Action Plan and Roadmap), Cyber Awareness Breakfast Conference Series, Cyber Range (Real World Training Center), and Resource Center for State Cybersecurity (Michigan co-chaired, NGA sponsored national partnership) was designed, implemented and made operational between March 2011 and November 2012. It brought together disparate security functions and created a new entity to enable further technology innovation using a comprehensive, metrics-based approach to reducing physical and cyber risks.

When was this project implemented or last updated? (Please specify month and year.) Has it incorporated new technologies and/or other innovations since its initial deployment? (In 300 words or less.)

A. This five-stage project was implemented in April to November 2011 and has been updated continually. Major updates, explained in question 8 and subsequent questions include: Establishing a Cross-boundary Partnership Framework (October to November 2012) 2011; Michigan Cyber Summit (October 7, 2011); Michigan Cyber Initiative (October 7, 2011 on-ward See Q11); Michigan Cyber Awareness Breakfast Conference Series 2012 - May to November 2012; Implementing the Michigan Cyber Range (November 2012 onward See Q11); Establishing the Resource Center for State Cybersecurity (October 2, 2012 onward See Q11). B. Refinements in core functions include: Basic Management Integration: The project included over sixty state staff and 400 contractors coming together with physical security and cyber-security directors reassigned to report to the new Chief Security Officer. Updates included: Joint exercises such as CYBERSTORM and NLE. Cross training staff across physical and cyber domains on emergency situations. Mid-range, operational IT/Physical integration. This phase brought newly-integrated identity management, technology integration into smart buildings, video integration and other benefits. Developed strategies and operational approaches for more effective management of "stealth threats" and the implications of cloud computing to business operations. Strategic cyber-infrastructure and public capital investments: Strategies such as securing the smart grid, strengthening health IT, modernizing public safety communications and intelligent transportation are ongoing efforts. Aligned with Federal, CIO and NASCIO priorities, including: budget and cost control; security enhancement tools; cloud computing; consolidation; virtualization, shared services and solutions. Addressed new compliance requirements for health IT. Next Generation Cyber Security Awareness Training: Over 47,000 Michigan State Government Employees have now received their first of twelve cyber security awareness training lessons, with over 81% participation. By the beginning of February 2013, this will be true for all state employees. Employees will receive one lesson every other month for 24 months.

If this is a previously submitted project that has been significantly updated and/or expanded, please describe the nature of the update here. (In 300 words or less.)

The project has not been submitted previously. However, the project was a finalist in the 2012 NASCIO Recognition Awards: NASCIO Honors Outstanding Information Technology Achievements Integrating Cyber and Physical Security: Ending the Divide Using a Comprehensive Approach to Risk Detail is available at http://www.nascio.org/awards/nominations2012/2012/2012MI10-NASCIO%20Security%20Award%202012%20-%20Michigan%20FINAL.pdf

Is implementation of the project complete? If no, please describe the project's phases and which phase the project is now in. (In 300 words or less.)

1-3 of the five stages are fully implemented and operational. 4-5 have been implemented with additional deliverables anticipated. 1. Cross Sector Assessment (April-September 2011 Q5). 2. Merge Physical and Cyber-Security Functions (September 2011- Q5); Cross-boundary Partnership Framework (October-November 2012); 2011 Michigan Cyber Summit (October 7, 2011) http://events.esd.org/MichiganCyberSummit2011.aspx. Michigan is developing a cyber-command center and "cyber-defense response teams." This project was launched at the Michigan Cyber Summit, which was the national kickoff for Cybersecurity Awareness Month in October 2011 with Secretary Napolitano and Howard Schmidt speaking with Governor Rick Snyder. Michigan Cyber Initiative (October 7, 2011 on-ward See Q11) http://www.michigan.gov/documents/cybersecurity/MichiganCyberInitiative2011_365631_7.pdf http://www.michigan.gov/cybersecurity. Michigan Cyber Awareness Breakfast Conference Series 2012 - May to November 2012. The Breakfast Conference Series provided updates to the Cyber Initiative to citizens, business and industry. http://events.esd.org/. Michigan Cyber Range (November 2012 onward - Q11). Partnered with and Hosted by Merit Network, the Michigan Cyber Range enables individuals and organizations to develop detection and reaction skills through simulations and exercises. The program offers students and IT professionals a full curriculum of meetings and workshops as well as critical cyber-security training and awareness tools. http://www.merit.edu/news/newsarchive/article.php?article=20121109_ cyberevent. 5. Resource Center for State Cybersecurity (October 2, 2012 onward Q11) Governor Snyder will be co-chairing the National Governors Association's "Resource Center for State Cybersecurity" with Governor O'Malley of Maryland. This resource center will develop comprehensive cyber security strategies for use by all fifty states by providing guidelines for the protection of our ever-growing technology ecosystem. Governors will be given the tools to address expanding cyber threats.

Please provide at least one example of how the technology project has benefited a specific individual or organization. Feel free to include personal quotes from individuals who have directly benefited from the work. (In 300 words or less.)

Benefits accrue to a wide range of individuals and organizations at the state and national levels and include direct services and cost avoidance as well as improved alignment of policies, strategies and operations. Michigan Operations: Plans completed for Security Operations Center (SOC), Rapid Cyber Defense Response Team (Public/Private), and new Michigan Cyber Command Center The development of a comprehensive security strategy (see Michigan Cyber Initiative) for all Michigan resources and infrastructure (completed and launched on October 2011). New architecture for access cards, improved video surveillance, business continuity and data center security. State Agencies: Agency projects completed more securely included: PCI Compliance & IRS audit findings closed (Treasury), health information sharing efforts (Community Health). New Joint Cyber Command Center collocated with Michigan State Police Hard Savings of $500,000 on emergency management staffing functions and potentially millions in avoidance through improved, integrated security. Universities: New Michigan Cyber Range in partnership with universities this public/ private partnership is a test bed for testing global cyber threats and solutions. Strategic and Operational Alignment (National): Enhanced National Partnerships with FBI, InfraGard, DHS and MS-ISAC. First State to launch "Albert" Intrusion Detection System with MS-ISAC. Coordination role on DHS Government Coordinating Council for NASCIO. (One outcome led to State CIOs being briefed by NSA on threats.) Next Generation Cyber Security Awareness Training: Over 47,000 Michigan State Government Employees have now received their first of twelve cyber security awareness training lessons. Local Governments: Training is also available to local units of government. The Michigan Court of Appeals, Supreme Court, MEDC, Office of the Auditor General and several others have already signed up to participate. Citizens and Business:

The Michigan Cyber Initiative Toolkit contains a set of resources to help insure online safety practices for citizens and business.

Would this project be considered an innovation, a best practice or other notable advancement that could be adopted by or tailored for other organizations and uses? If yes, please describe that here. (In 300 words or less.)

Michigan is the first state to merge physical and cyber-security on an enterprise-wide basis. This model reduces risk and delivers better security with fewer resources by eliminating overlapping duties. Specifically, this approach offers greater executive visibility, creates operational efficiencies, improves risk management, provides streamlined incident management if breaches occur, maximizes existing investments and reduces operational costs. New metrics, processes and procedures have been established across multiple agencies and domains to better coordinate and communicate activities. Our model offers tiers that are easily adaptable to other states, and several states have made inquiries, including on the Cyber-range. Michigan's history of participation and innovation in security initiatives is an indicator that the state has a sustained innovation and leadership role. Two years ago Michigan participated in a proof of concept of the federal government's Einstein traffic monitoring system that was eventually turned over to the Multi-State Information Sharing and Analysis Center. As a result of its participation in Einstein, Michigan resolved 40 malware incidents affecting 590 state devices. Michigan also recently appointed a chief security officer, a first-of-its-kind position among state governments that will combine oversight of computer and physical infrastructure. Another asset is that five Michigan colleges and universities are designated by the National Security Agency as National Centers of Academic Excellence in Information Assurance. Besides the creation of the new cyber-command center, the state's cyber-security initiative will also attempt to improve curricula for cyber-security in schools and provide economic development opportunities for the cyber-security industry. A full version of the Michigan Cyber Initiative, as well as a new cyber-toolkit, can be found at http://www.michigan.gov/cybersecurity.

If there are any other details that the judges should know about this project, please note them here. (In 300 words or less.)

Supplemental detail on stages 3, 4 and 5: 3 - Cyber Initiative: State Police "Cyber Command Center" to coordinate efforts of cyber emergency responders. Cyber Defense Response Team to support state government and key stakeholders. Provide a collaborative task force for sharing homeland security information through the 24/7 Michigan Intelligence Operations Center (MIOC). Develop a curriculum focused on enhancing the overall advancement of cybersecurity. Accelerate the economic development and growth of the cybersecurity industry, providing innovative economic development opportunities. Provide online toolkit for safeguarding homes, businesses, government, schools. Support the Michigan Attorney General's Cyber Safety Initiative (CSI) for children in K – 8. 4 - Michigan Cyber Range The Cyber-Range will enhance Michigan's protection of computer systems and sensitive data by pairing cybersecurity resources -- a full curriculum of meetings and workshops, and critical cybersecurity training and awareness tools -- with hands-on training opportunities. The range helps individuals and organizations develop detection and reaction skills through simulations and exercises. Critical areas that will benefit from the creation of the Michigan Cyber Range include: infrastructure defense; homeland security; criminal justice and law enforcement; academic and educational programs and curricula related to information and communications technology; and entrepreneurial, small and medium businesses. 5 - Resource Center Phase 1 - Leverage resources, identify issues, develop recommendations for states: Convene planning group to help inform and plan project activities; Commission white papers on cyber-security for an audience of governors and state policymakers; Create National Policy Council on State Cybersecurity; Produce governors' guide and policy framework; Disseminate project findings; Provide technical assistance to governors. Phase 2 - Identify states in which to implement the recommended courses of actions.