FEMA

Sharing Information
Enhancing Preparedness
Strengthening Homeland Security

Lessons Learned
Information Sharing
LLIS.gov

DISCLAIMER *Lessons Learned Information Sharing (LLIS.gov) is the Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the emergency management and homeland security communities. The Web site and its contents are provided for informational purposes only, without warranty or guarantee of any kind, and do not represent the official positions of the Department of Homeland Security. For more information on LLIS.gov, please email feedback@llis.dhs.gov or visit www.llis.gov.*

LESSON LEARNED

Cybersecurity: The Michigan Cyber Disruption Response Strategy

SUMMARY

The *Lessons Learned Information Sharing (LLIS.gov)* research team identifies lessons learned derived from real-world or exercise experiences within the whole community and documents these lessons for emergency managers to consider when developing plans and exercises. In response to the growing threat of cyber attacks to the State of Michigan, a coalition of public and private sector partners developed and implemented a new framework for addressing cyber challenges. As a result, Michigan released the Michigan Cyber Initiative (the Initiative) in October 2011, followed by the Michigan Cyber Disruption Response Strategy (the Strategy) in September 2013. This holistic, partnership-based approach improved the State's overall cybersecurity posture, and provides a valuable example for other jurisdictions to consider in their own cyber response framework development.

Whole community participants contributed to the development of the Michigan Cyber Disruption Response Strategy *(Source: Michigan Cyber Disruption Response Strategy. September 16, 2013.)*

DESCRIPTION

In 2010, the Michigan state government experienced a high volume of cyber attacks, blocking nearly 30,000 web browser attacks every day, while the U.S. Government only registered an average of 15,000 cyber attacks a day against Federal IT systems. At this time, Michigan's emergency preparedness response plans focused on "traditional" hazards such as tornadoes, fires, and floods and lacked an effective strategy for sharing information with public or private sector partners during a cyber emergency. As a result, the state developed a cyber response framework consisting of two components, the Michigan Cyber Initiative and the Michigan Cyber Disruption Response Strategy.

Michigan's Cyber Initiative outlined goals for protecting state government, businesses, and critical infrastructure from cyber attacks. Then a public-private partnership developed and executed the Michigan Cyber Disruption Response Strategy.

LLIS.gov defines a Lesson Learned as a positive or negative experience derived from an actual incident, operation, training, or exercise obtained from a validated After Action Report or interview.

Public-Private Partnership in Strategy Development

Goals of the Michigan Cyber Disruption Response Strategy

Goal 1: Improve situational awareness among critical infrastructure owners and operators through enhanced communication and collaboration regarding cyber threats.
Goal 2: Create specific plans, as annexes to the strategy, for the prevention and mitigation of, response to, and recovery from cyber disruption events affecting critical infrastructure owners and operators by 2014.
Goal 3: Train key staff and exercise communication and response plans developed in accordance with this strategy annually, beginning in 2013.
Goal 4: Conduct thorough risk assessments to identify the vulnerabilities of Michigan's critical infrastructure to cyber attack.

Michigan's private sector partners were instrumental in developing the Strategy and supporting its long-term success. The State's newly appointed Chief Information Officer (CIO) established connections with private sector CIOs—many of whom worked for Fortune 500 companies—and solicited advice on key cybersecurity strategies through monthly meetings. In 2012, the Michigan Chief Security Office (CSO) also began meeting monthly with CSOs and Chief Information Security Officers (CISOs) from the private sector and state government agencies. Michigan officials began referencing these groups as the "CIO Kitchen Cabinet" and the "CISO Kitchen Cabinet." After sharing best practices and attending conferences with his peers, Michigan's CSO realized the State lacked the capability to effectively handle a statewide cyber emergency involving key critical infrastructure. In light of this, the State began work on the creation of the Strategy.

The Kitchen Cabinet groups developed a network of stakeholders invested in the Strategy. Both Cabinets collaborated with statewide planners and provided government and private sector subject matter experts to:

- Address gaps in the Strategy ahead of planned revisions in Fiscal Year 2015–18;
- Properly account for all necessary structures, agencies, and whole community entities necessary for a state response to a cyber emergency;
- Assess gaps in existing cyber capabilities via an enterprise risk assessment; and
- Identify existing capabilities used in response to physical disasters that could also be used in response to a cyber attack.

This approach enabled the State to effectively collaborate with the private sector and ensure whole community best practices and strategies informed Michigan's overall Cyber Disruption Response Strategy.

Implementing the Strategy

State leaders implemented the 2014-2016 Michigan Training and Exercise Plan to ensure the Strategy was properly executed. This plan required all Michigan State employees to update their basic cyber training. Senior leaders within Michigan's government prioritized completing their training to set a precedent for other state workers. Similarly, these leaders began participating in all statewide cyber-related training activities and tabletop exercises. These actions sent a strong message to all State employees about the importance of cyber training and increased overall awareness of cybersecurity issues.

Between 2010 and 2012 Michigan also improved its emergency preparedness and cybersecurity training exercises. For example, planners incorporated new cyber threat elements into exercises and state officials directed offices to incorporate lessons learned from each exercise into future exercises. In addition, Michigan is planning to conduct more cyber exercises in the future to continuously improve the State's response capabilities.

The Strategy is also transforming Michigan's cybersecurity awareness training. The training program has evolved from a PowerPoint-style program into a modern platform, incorporating popular learning principles like gamification and interactive content.[†] Further, the training program expanded to include tools for whole community groups, such as citizens, small businesses, households, technical staff, and others.

Michigan's Cyber Defense Response Team

Leaders in Michigan created the Michigan Cyber Defense Response Team to provide ongoing support to the state government and key stakeholders. This team functions under the operational control of the Michigan Cyber Command Center (MiSOC), and undertakes several key programs—including a response network that uses a "train the trainer" approach—to inform stakeholders, improve network security, and promote training and operational process standards. Proactively defending against cyber threats ensures the best-of-class cyber emergency response and is an important component of state leadership efforts to meaningfully support and implement the new Strategy statewide.

RECOMMENDATIONS

The success of Michigan's cyber response framework demonstrates the importance of bringing private and public partners together to improve cybersecurity capabilities at all levels. Similarly, the use of "Kitchen Cabinets" that include private sector partners can provide needed expertise to address capability gaps and incorporate innovative practices into the development and implementation of a cyber response framework.

REFERENCES

Daniel Lohrmann, Chief Security Officer for the State of Michigan. Personal Interview. March 10, 2014.

State of Michigan. Michigan Cyber Disruption Response Strategy: Protecting Michigan's Critical Infrastructure and Systems. September 16, 2013. https://www.llis.dhs.gov/content/michigan-cyber-disruption-response-strategy.

State of Michigan. Michigan Cyber Initiative: Defense and Development for Michigan Citizens, Businesses and Industry. October 2011. https://www.llis.dhs.gov/content/michigan-cyber-initiative.

[†] "Gamification" involves the application of thinking, mechanics, and features from games—often video games—to non-game problems like social challenges, business strategies, and learning modules. It is intended to engage users in problem solving, learning difficult or complex content, and motivating other behavioral changes.