Cyber Security

Michigan's Landscape

Dan Lohrmann, Michigan Chief Security Officer
April 29, 2013

2012

- 31.5 million malware removals from e-mail
- 24.5 million spam e-mails blocked per month
- 2.1 million web browser based attacks
- 142 million http based attacks
- 24.5 million network scans
- 1.2 million intrusion prevention blocks

- 17 Agencies
- 48,000+ State Employees
- 800 Critical Business Functions
- 64,000+ Computing Devices

Michigan's Centralization Story

Centralized IT Strategy
- Network, mainframe, data warehouse, data centers

Centralized IT Security Strategy
- Security architecture
- Perimeter defense
- Security tools and training
- Enterprise security framework
- Enterprise PCI Compliance

NIST Model

Security Convergence – 2011
- Michigan Chief Security Officer

Combined Physical and Cybersecurity
- One CSO, one organization

Operational Efficiencies
- Camera systems, monitoring, ID processing, emergency management

Communication
- One team, one voice

What We've Done

- **Governor's "Michigan Cyber Initiative"**
  - 2011 Michigan Cyber Summit (National kickoff event)
  - 2012 Cyber Breakfast Conference Series
  - 2013 Michigan Cyber Summit (in planning stage)
- **Michigan Cyber Security Toolkit**
  - User Guides for Business, Government, School, Home
  - Monthly newsletter to private/public partners
- **New Cyber Awareness Training for State Employees**
- **Michigan Cyber Range**
  - Training/testing facility with private/public partners, opened November 2012

www.michigan.gov/cybersecurity

Where We're Going

Michigan Security Operations Center (MiSOC)

- Enhancing current operations to 24x7x365 monitoring and detection

Michigan Cyber Defense Response Team (MCDRT)

- Developing "Catastrophic Cyber Disruption Plan" for public/private partners
- Team of experts deployed in the event of a major incident

Michigan Cyber Command Center (MCCC)

- Partnering with law enforcement and MIOC for intelligence sharing
- Include components of MiSOC and MCDRT

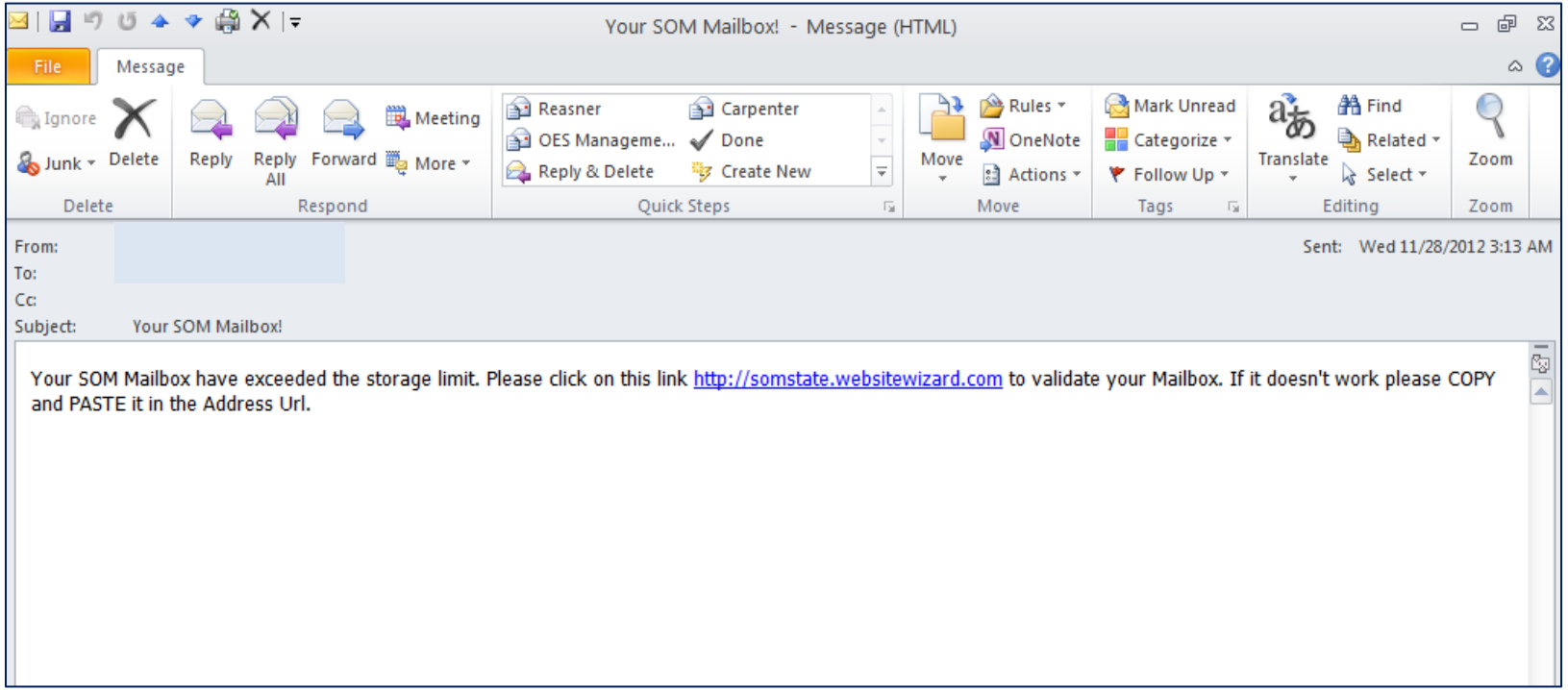
Michigan Cyber Range

- Training classes began March 2013

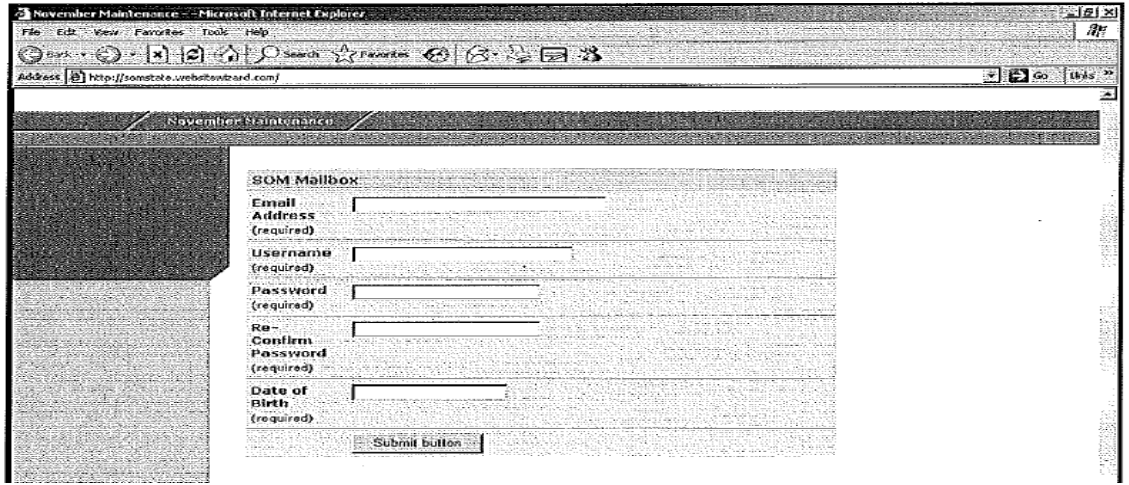
Our valued partners include:

- **Department of Homeland Security (DHS)**
- **Multi-State Information Sharing & Analysis Center (MS-ISAC)**
- **Michigan Intelligence Operations Center (MIOC)**
- **Federal Level Emergency Exercises**
  - ✓Cyber Storm I, II, III, and IV
  - ✓NLE 2012 Tabletop and Exercise
- **Federal, State and Local Law Enforcement**
  - ✓Michigan State Police
  - ✓FBI
  - ✓US-CERT

One True Story: A Sophisticated Spearphish . . .



Resulting screen requests user's e-mail credentials . . . with fake "Submit" button (credentials transmitted upon entry into text box) .



Three Pieces of Low-Hanging Fruit to Kick-start Action

1. Start with boats already leaving the dock (or projects that are already funded).

2. Utilize Payment Card Industry (PCI) Compliance, health regulations (HIPAA), or other mandates to drive security actions.

3. Leverage Information Technology Infrastructure Library (ITIL) and other infrastructure initiatives to strengthen security efforts.