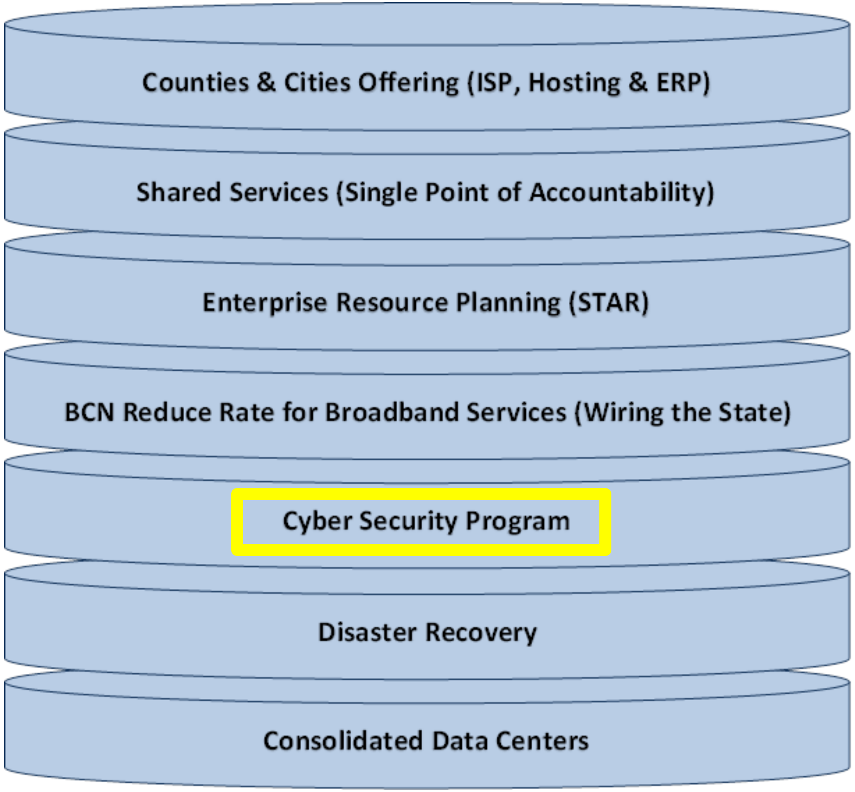
4th Annual Cyber Security Summit Madison, WI.

PRESENTER: DAVID CAGIGAL

October 27, 2016

DET Strategic Enterprise Solution Set



Counties & Cities Offering (ISP, Hosting & ERP)

Shared Services (Single Point of Accountability)

Enterprise Resource Planning (STAR)

BCN Reduce Rate for Broadband Services (Wiring the State)

Cyber Security Program

Disaster Recovery

Consolidated Data Centers

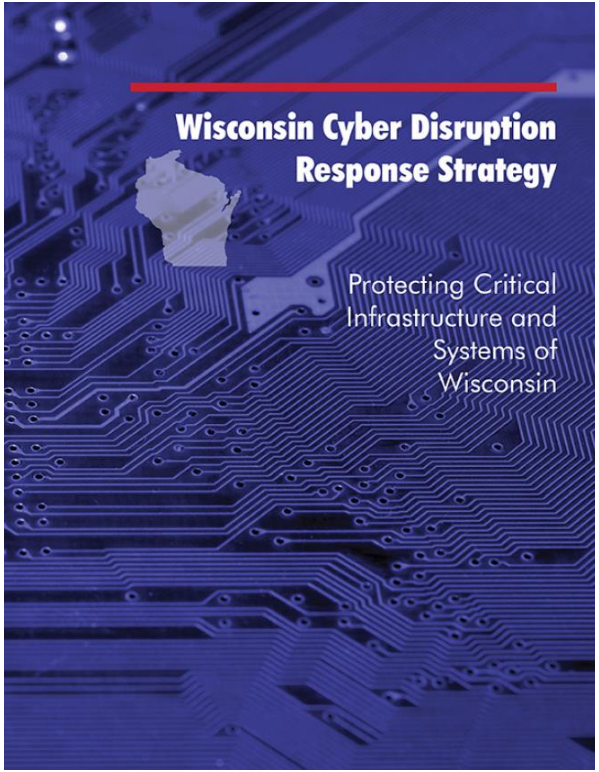
IT Strategy

Cybersecurity

- **Education, Awareness, and Training** – cultivate a security awareness culture within Wisconsin state agencies by providing continuous training and educational opportunities.
- **Security** – promote an evolutionary change through the development of an effective vulnerability management program to mitigate risks and to ensure State of Wisconsin IT systems are configured appropriately and securely.
- **Wisconsin Cyber Disruption Response Strategy** – use the Cyber Disruption Response Strategy as a guide for communications, training, response, and recovery of operations, in addressing probable infrastructure disruptions resulting from cyber intrusions or attacks. We must protect the state’s infrastructure, both public and private.
- **IT Disaster Recovery (ITDR)** – deploy a strategy to ensure the continuity and resilience of enterprise IT services.

Wisconsin Cyber Disruption Response Strategy

- 16 Critical Infrastructure/Key Resource Sectors that must be protected.
- Centered on these sectors, State of Wisconsin has developed a Cyber Disruption Response Strategy in a Public/Private Partnership.
- **A well defined plan is under development with WEM (Wisconsin Emergency Management), which will replace our current cyber annex. This new plan will become the "Cyber Incident Response Annex."**



Wisconsin Cyber Disruption Response Strategy

Protecting Critical Infrastructure and Systems of Wisconsin

16 Critical Infrastructure/Key Resources

Chemical 	Commercial 	Communications 	Manufacturing
Dams 	Defense 	Emergency 	Energy
Financial 	Food & Ag 	Gov Facilities 	Healthcare
IT 	Nuclear 	Transportation 	Water

Cyber Disruption Response Strategy

Goals/Objectives

1.Governance Authority

- To establish a consistent cyber disruption response governance authority and strategy
- Establish decision points mapped to the lifestyle of an event, and determine threat level, action plans, and resource allocations

2.Organization, Roles & Processes

- Each sector will identify, protect, detect, respond, and recover from any large-scale or long duration cyber disruption.

3.Risk Profile and Capacity

- Conduct thorough risk profiles to identify the vulnerabilities of Wisconsin’s critical infrastructures to cyber attack.

4.Communications

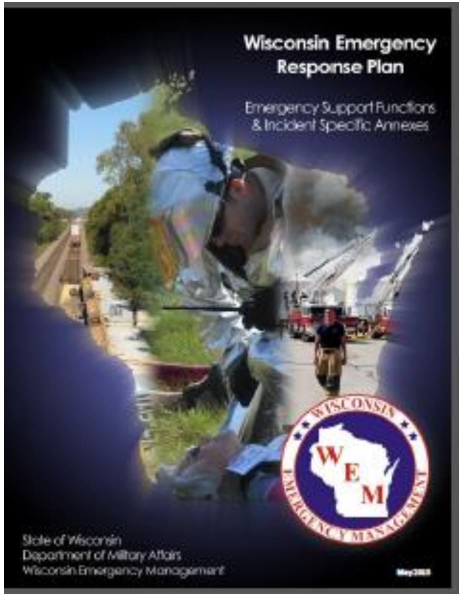
- Improve communication among cooperating critical infrastructure owners and operators.

5.Response Recovery

- Train key staff and exercise communication and response plans developed in accordance with this strategy annually.

Cyber Incident Response Annex

- The Wisconsin Emergency Response Plan (WERP) is a comprehensive all-hazards plan, which provides for a statewide program of emergency management.
- Cyber Incident Response Annex:
  - Is an element of the WERP
  - Establishes a standardized, flexible, and scalable foundation for state agency preparation for, and response to a threat or attack involving state networks, local government networks, and networks involved in supporting critical infrastructure
  - Provides guidance to state agencies regarding mitigation, prevention, protection, and response to actual or potential cyber-related threats and attacks
  - Provides guidance to counties, tribes, and local units of government regarding available state assets and resources



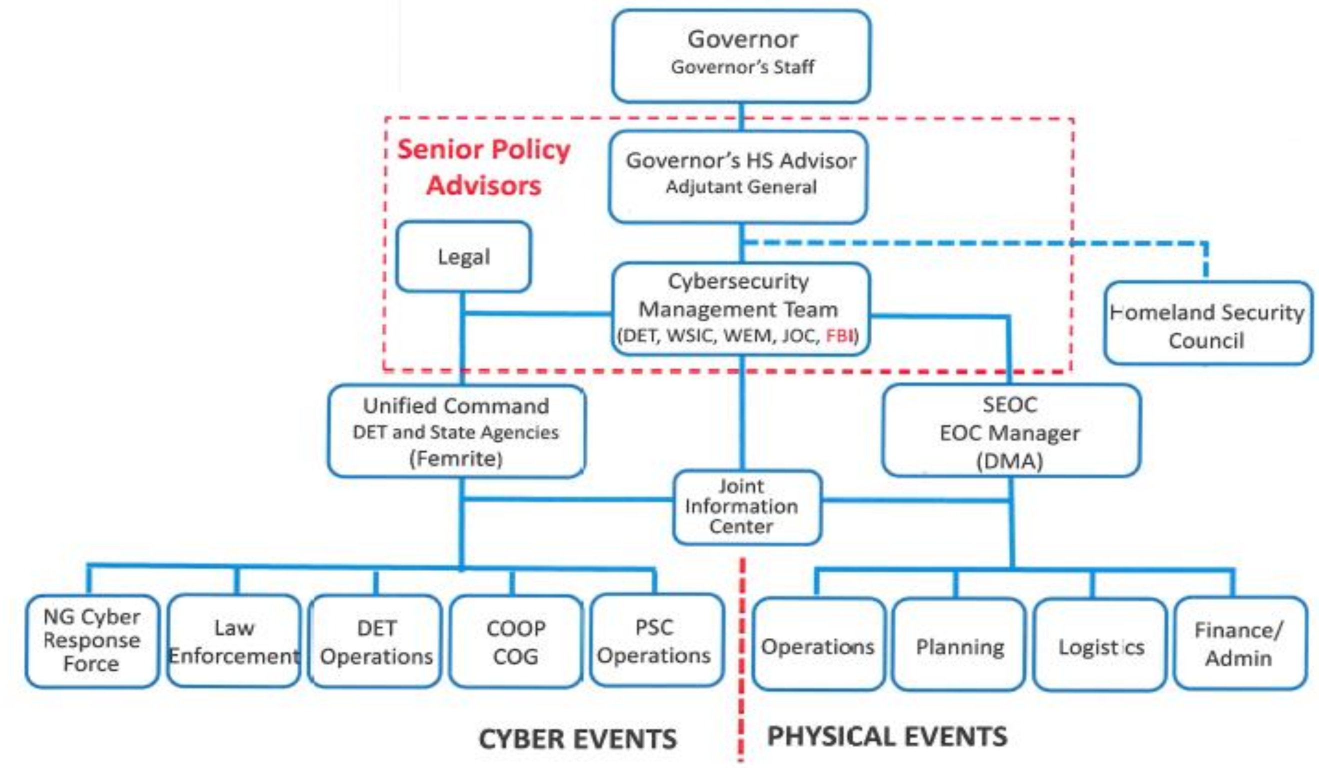
Wisconsin Emergency
Response Plan

Emergency Support Functions
& Incident Specific Annexes

State of Wisconsin
Department of Military Affairs
Wisconsin Emergency Management

May [illegible]

Coordination: Cyber & Physical Responses



Governor
Governor's Staff

Senior Policy Advisors

Governor's HS Advisor
Adjutant General

Legal

Cybersecurity Management Team (DET, WSIC, WEM, JOC, FBI)

Homeland Security Council

Unified Command
DET and State Agencies
(Femrite)

SEOC
EOC Manager
(DMA)

Joint Information Center

NG Cyber Response Force

Law Enforcement

DET Operations

COOP COG

PSC Operations

Operations

Planning

Logist cs

Finance/ Admin

CYBER EVENTS

PHYSICAL EVENTS

Focus: Maintain Critical Public Services and Support Law Enforcement Activities by Others

SLTT Teams

(Focus: Prevention to Recovery)

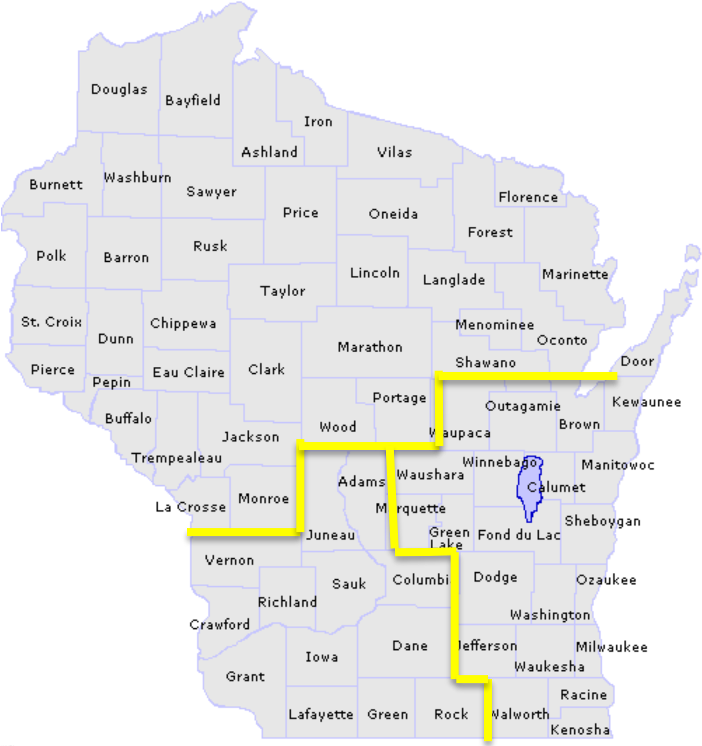
- Prevention
  - Penetration Testing
- Protection
  - Tools Techniques and Procedures
- Mitigation
  - Backup Strategy / Systems
- Response
  - Bench Strength
- Recovery
  - Bringing systems back to normal

Law Enforcement

(Focus: Enforcement of law and prosecution)

- Tools
  - Subpoenas, warrants, court orders
  - Investigative skills
  - Seizure
  - Apprehension and arrest
- Digital Evidence
  - Preservation
  - Prevent Contamination
  - Chain of Custody
  - Forensic Examination

Cyber Response Team Assignment



Team 1: Southeast and East Central

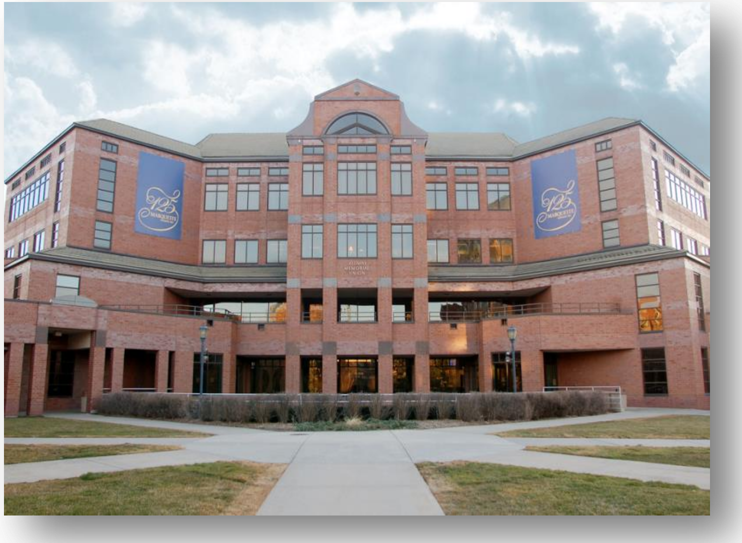
Team 2: Northwest, Northeast, West Central

Team 3: Southwest

SLTT Cyber Response: Cyber 15-1 & Cyber 15-2

September 8-9th, Ft. McCoy Wisconsin
Wisconsin Military Academy

October 27-28th, Milwaukee Wisconsin
Marquette Alumni Memorial Union



SLTT Cyber Response: Cyber XVI (16) & TTX

November 14-15th, Ft. McCoy Wisconsin
Wisconsin Military Academy

September 21st, Madison Wisconsin
Armed Forces Reserve Center

Training & Exercise: Apply Lessons Learned from SLTT

Future Plans – Civil Corps

•Continue to identify 16 CI/KR Private Sector Cyber-Response Teams

•Facilitate credential achievements

•Continue to develop joint training exercises with public and private cyber-response teams

•Coordinate a public and private cyber-response plan

THANK YOU!

David Cagigal, CIO

State of Wisconsin

Department of Administration

Division of Enterprise Technology