MUNICIPAL ELECTRIC UTILITIES OF WISCONSIN CYBERSECURITY SUMMIT

BILL NASH

CHIEF INFORMATION SECURITY OFFICER / DIRECTOR, BUREAU OF SECURITY,

STATE OF WISCONSIN, DEPARTMENT OF ADMINISTRATION, DIVISION OF ENTERPRISE TECHNOLOGY

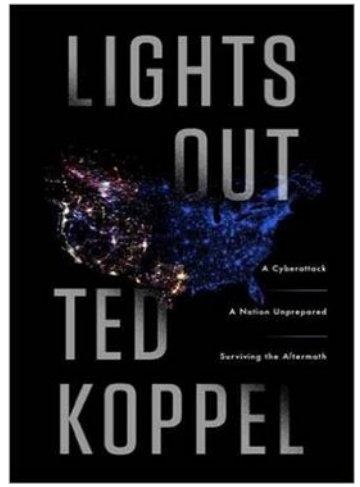
STATE OF WI CYBER STATISTICS

- 605 Million Filtered Emails
  - 532 Email Phishing Incidents
- 36 Million Vulnerability Scans
- 93,000 Preventive Malware Downloads
- 41,000 Attempts to Exploit Web Apps
- 108,000 Attempts to Break Passwords
- 32,000 Blocked Malicious Internet (IP) Addresses

WISCONSIN DEPARTMENT OF ADMINISTRATION DOA.WI.GOV

WHY ME? - CYBER ATTACK MOTIVES

- **Criminal Activity**
  - Make Money
- **Social Action**
  - Make a Statement/Protest
- **Global Economic Espionage**
  - Steal trade secrets, etc.
- **Cyber Warfare**
  - Attacks on infrastructure, etc.



WISCONSIN DEPARTMENT OF ADMINISTRATION DOA.WI.GOV

CYBER IN THE NATIONAL NEWS

- Colorado, DOT
- City of Atlanta, Georgia
- Jackson County, Georgia
- City of Baltimore, Maryland
- 22 Municipalities, Texas

WISCONSIN DEPARTMENT OF ADMINISTRATION DOA.WI.GOV

COST OF A DATA BREACH

2018 Cost of a Data Breach Study by Ponemon -

Global average cost of a data breach $3.86 million ($148 / record)

- Notification
- Credit Monitoring
- Regulatory Fines/Penalties
- Investigation/Forensics
- Downtime/Loss of Productivity
- Loss of Citizens'/Customer Confidence

WHAT DO WE DO ABOUT IT?

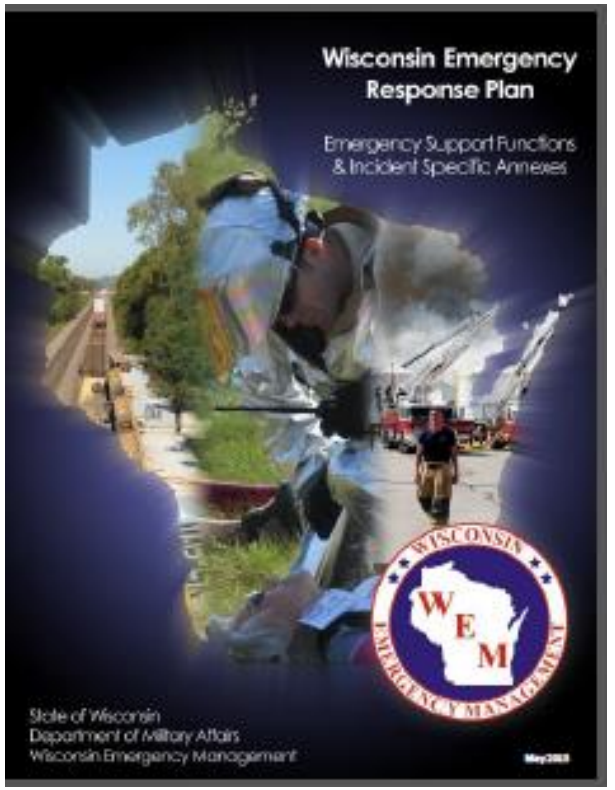
"It takes a network to defeat a network."

Gen. Stanley A. McChrystal (2011)

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



DEPARTMENT OF ADMINISTRATION
DOA.WI.GOV

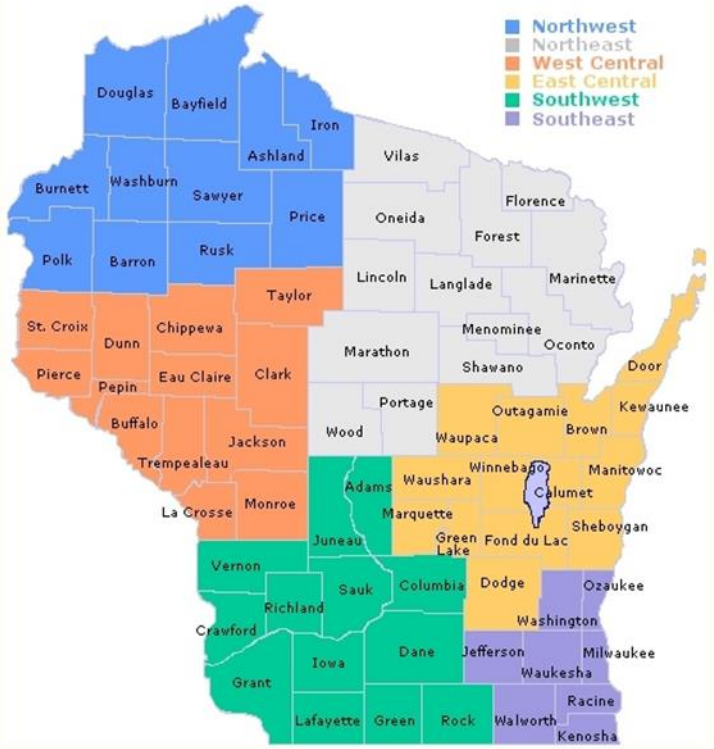
CYBER RESPONSE TEAM (CRT)

- US Department of Homeland Security Grant Funding
  - Initiated in 2015
  - Provides training to local government CRT members
  - Growing a cyber response capability for Wisconsin

LOCAL GOVERNMENT CYBER RESPONSE TEAMS (CRT)

Teams assigned to Wisconsin Emergency Management regions:

- **Team 1**: Southeast and East Central
- **Team 2**: Northwest, Northeast, West Central
- **Team 3**: Southwest



WISCONSIN DEPARTMENT OF ADMINISTRATION DOA.WI.GOV

STATEWIDE SUPPORT TEAMS 4 AND 5

Team 4 – Statewide

WI National Guard Team - Supplements other teams

Team 5 – Statewide

Team is Private Sector Based – Representatives are from the following Companies:

- Alliant Energy
- Nextera Energies
- WE Energies
- MG&E (Madison Gas and Electric)
- American Transmission Company
- AT&T Communications
- Cisco
- 5Nines

CYBER EXERCISES

2015

September 8-9th, Ft. McCoy Wisconsin

October 27-28th, Milwaukee Wisconsin

2016

September 21st, Madison Wisconsin

November 14-15th, Ft. McCoy Wisconsin

2017

Nov. 8-9, 2017, Madison Wisconsin

2018

Mar. 20-23, 2018 Madison Wisconsin

May 15-16, 2018 Cudahy Wisconsin

(Dark Sky participation)

2019

September 11-12

Madison, WI.

CRT IN ACTION

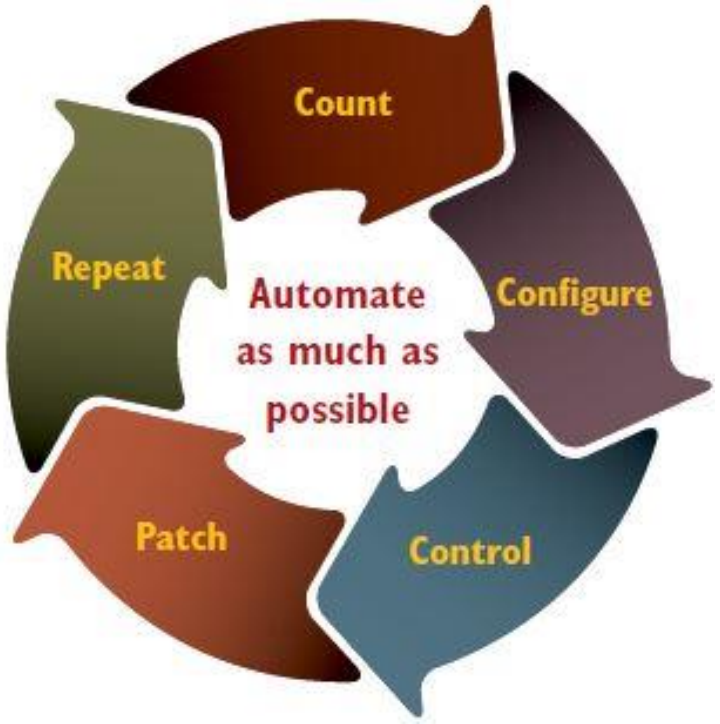
Response to multiple incidents in Wisconsin disrupting services.

- **Social Action**
  - Doxing of Public Officials and Law Enforcement
  - Swatting
  - DDoS
- **Cyber Crime**
  - Ransomware
  - Phishing
  - Web Site Defacement

BASIC PREVENTION – CYBER HYGIENE

Cyber Hygiene

- Know what you have
- Install patches / updates
- Follow secure configuration best practices
- Repeat



WISCONSIN DEPARTMENT OF ADMINISTRATION DOA.WI.GOV

BASIC PREVENTION – OTHER GOOD PRACTICES

- **Authentication and Access Control** (Strong PW, Least Privilege, MFA, etc.)
- **Backups** (test restores, data, images, RPO, RTO)
- **Plans** (IR, DR, COOP)
- **Security Awareness Training Program**
- **Beyond basic?** NIST 800.53, CIS Critical Security Controls

RESOURCES

Oh yes, it's free!

(Included in Tax $)

- WSIC and CRT
- Multi-State – Information Sharing and Analysis Center (MS-ISAC)
- Cybersecurity and Infrastructure Security Agency
- FedVTE – Federal Virtual Training Environment

CYBER INCIDENT ASSISTANCE

Cyber Incident:

WEM Duty Officer

800-943-0003