League of Wisconsin Municipalities

October 18, 2017

Bill Nash
Chief Information Security Officer
State of Wisconsin, Department of Administration, Division of Enterprise Technology

The State Target

2

5.7 Million Citizens

Applications and Data such as
- Birth Certificates
- Tax Returns
- Personal Health Information
- Drivers Licenses
- Worker's Compensation
- ETC.

40,000 Employees – A.K.A. Phishing Targets
- Stolen Credentials
- Downloaded Malware

47,000 Endpoints Connected
- Laptops/PCs/Cell Phones/etc.

State Cyber-security Statistics for 2016 - 2017

3

1.2 Billion Malicious Emails
- 25K per employee per month
- 95% of all incoming emails

9 Million Vulnerability Scans

40,000 Potential Malware Downloads

42,000 Attempts to Exploit Web Applications

505,000 Attempts to Break Passwords

Cyber Attack Motives

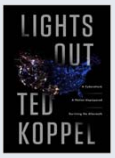
4

Criminal Activity
- Make Money

Social Action
- Make a Statement/Protest

Global Economic Espionage
- Steal trade secrets, etc.

Cyber Warfare
- Attacks on infrastructure, etc.



Common Attack Types

5

- **Social** – deception, manipulation, intimidation, etc., to exploit the human element, or users, of information assets (and which is typically a precursor to hacking and malware)
- **Malware** – any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent
- **Hacking** – attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms
- **Denial of Service** – any attack meant to shut down a machine or network, making it inaccessible to its intended users

Hacking: Man-In-The-Middle

6

Malware: Ransom

7

Social: Phishing Email

8

@cfp.ufrb.edu.br

From: ESSWI2@wisconsin.gov [mailto:mestrado.campo@cfp.ufrb.edu.br]
Sent: Friday, January 22, 2016 9:35 AM
Subject: IMPORTANT TAX RETURN DOCUMENT AVAILABLE

Dear Account Owner,

Our records indicate that you are enrolled in the State of Wisconsin paperless W2 Program. As a result, you do not receive a paper W2 but instead receive e-mail notification that your online W2 (i.e. "paperless W2") is prepared and ready for viewing.

Your 2015 W2 corrected statement is ready for viewing, follow the link below

Click Here to Login

To opt out of the Paperless W2 Program, please login to Employee Self Service at the link above and go to the W2 Delivery Choice webpage and follow the instructions.

State of Wisconsin Human Resource Management Systems

Social: Fake WI ESS Web Site

9

www.flirtingvision.co.nz/css/wisconsin/esslogin.htm

Cost of a Data Breach

10

Ponemon Institute's "2016 Cost of Data Breach Study: United States" released in June 2016

- Average cost for each lost or stolen record containing sensitive and confidential information $221.

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

What Can You Do?

11

- Security Awareness Culture
  - Use Secure Passwords
    - Use strong passwords that use a combo of words, numbers, symbols and both upper and lower case letters
    - Do not share your password
    - Use different passwords for every unique account such as work, banking and home email
    - Disable the "save password" feature in your internet browser
    - Use multifactor authentication when possible
  - Don't Take The Bait…
    - Do not open attachments or click on links from untrusted sources
    - Never send personal information in an email
    - Use work email address for work purposes only
- More help…

StaySafeOnline.org
Powered by National Cyber Security Alliance

What Can Your Organization Do?

12

- Take Care of the Basics
  - Protect Your DATA
    - Control access
    - Test backup and recovery
  - Patch (Servers, PCs, laptops, tablets, mobile phones)
    - Patches are no longer issued for non-supported systems.
    - Example: Windows 2003 End of Life Occurred on July 14, 2015. Only one week later, a new vulnerability was created and there is no patch to fix it.
- More help …

https://www.us-cert.gov/ccubedvp

US-CERT United States Computer Emergency Readiness Team
C3 VOLUNTARY PROGRAM

Services for Your Organization

13

MS-ISAC
Multi-State Information Sharing & Analysis Center

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

www.cisecurity.org/ms-isac/

Free Training

14

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT

The **Federal Virtual Training Environment** (FedVTE) is a system that provides U.S. government employees, members of the military, and veterans with free online training in multiple fields.

fedvte.usalearning.gov

What If You See Something?

15

CYBERATTACK
Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.

wiwatch.org

What Can We Do Together?

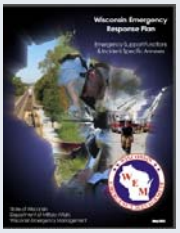
16

"It takes a network to defeat a network."
Gen. Stanley A. McChrystal (2011)

Cyber Incident Response Annex

17

- 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



Cyber Response Team (CRT) – Inception

18

- US Department of Homeland Security Grants:
  - $50k in 2015
  - $98k in 2016
  - Funding through August 30, 2018
- This program provides a 75% cost share to train local government CRT members.

CRT Assignment

19

Teams assigned to Wisconsin Emergency Management regions.

- **Team 1: Southeast and East Central (40% pending 50%)**
  - Wauwatosa
  - Wood County*
  - Pleasant Prairie
  - Manitowoc County
  - Milwaukee County
  - WI DOA
- **Team 2: Northwest, Northeast, West Central (100%)**
  - Sawyer County
  - Bayfield County (2)
  - Portage County
  - City of Eau Claire
  - City of Fond du Lac (2)**
  - La Crosse County
  - Eau Claire County (2)
- **Team 3: Southwest (50%)**
  - WI DOA
  - WI OCI
  - WI DOT
  - City of Madison
  - Fall River School District

* LMR/Dispatch Statewide
** GIPAW Statewide

Statewide Support Teams 4 and 5

20

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

21

2015
September 8-9th, Ft. McCoy Wisconsin
October 27-28th, Milwaukee Wisconsin

2016
September 21st, Madison Wisconsin
November 14-15th, Ft. McCoy Wisconsin

2017 - 2018
Nov. 8-9, 2017, Table Top
Feb. 5-9, 2018 Team Training
May 15-16, 2018 Dark Sky

CRT in Action

22

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

Questions?

23

For more information:
CRT@Wisconsin.gov

Cyber Incident:
WEM Duty Officer
800-943-0003