CYBER SECURITY

ARE WE SECURE YET?

2017 Wisconsin Digital Summit

YOUR PRESENTERS

- Bill Nash, CISO State of Wisconsin
- Allen Mundt, ISO and Infrastructure Administrator Waukesha County

PROBLEM STATEMENT

We want ***"Security"***,

But, how do we know when we get there?

Are We Secure Yet??

AGENDA

- Threat overview
- Staffing and Budget Realities
- Cyber Hygiene
- Technical Cyber Security Practices
- Human and Organizational Cyber Practices
- The Cavalry
- The Future

AI

CURRENT THREAT ENVIRONMENT

- Motives:
  - Social Action;
  - Criminal Activity;
  - Global Economic Espionage;
  - Cyber Warfare
- We are not Equifax, or Target or Yahoo, so why Government?
  - We require our constituents to provide information to get services.
  - We create, acquire, store and transmit large quantities of data everyday.
  - Some is public, but much has the highest privacy levels.
  - Names, address, SSN, phone numbers, legal, medical, birth, death, criminal justice, emergency services.
- Sensitive information with limited budget and limited resources to protect.

Bill

THE STATE TARGET

5.7 Million Citizens, 72 Counties, Countless Municipalities

Applications and Data such as

- Birth Certificates
- Tax Returns
- Personal Health Information
- Drivers Licenses
- Worker's Compensation
- Legal, Child Custody
- ETC.

40,000 Employees, at the State-Level Alone – A.K.A. Phishing Targets

- Stolen Credentials
- Downloaded Malware

47,000 Endpoints Connected

- Laptops/PCs/Cell Phones/etc.

…add to that all of the SLTT organizations in addition to the State

Bill

STATE CYBER-SECURITY STATISTICS FOR 2016 - 2017

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

Bill

COST OF A DATA BREACH

Ponemon Institute's "2017 Cost of Data Breach Study: United States" released in June 2017

- Average cost for each lost or stolen record containing sensitive and confidential information $141.

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

Bill

REALITIES WE FACE

- Fast-Changing Technologies. Software companies interested in functionality.
- Lots of adversaries
- Limited time
- Limited budgets
- Limited staff
- A single user action can defeat security
- We have to be right all the time

AI

"COMPUTER TIME"

- Short measure of human history - about 8000 years.
- Assuming usable computers since 1950, computers have existed for 8/10 of 1% of time.
- Public Internet since about 1993.
- Internet and related technologies for 3/10 of 1% of time.
- Consumer-driven
- Revolutionary, breakthrough, unprecedented, and…
- ***DANGEROUS***

REALITIES WE FACE

- Fast-Changing Technologies. Software companies interested in functionality.
- Lots of adversaries
- Limited time
- Limited budgets
- Limited staff
- A single user action can defeat security
- We have to be right all the time

AI

WHERE ARE THE ANSWERS?

- Nothing ensures 100% success
- Not if, …
- Nothing is iron-clad, but there are things you can and should consider.

AI

CYBER-HYGIENE

- Concept/term coined in several cyber security frameworks.
- Sets of policies, procedures, disciplines that create the "environmentals" necessary to reduce risk.
- Function at 2 levels:
  - Technical
  - Organizational

AI

TECHNICAL CYBER HYGIENE

- Those technologies and procedures which should be at least considered for baseline protections.
- Disciplines.
- The list is long and you may not do it all.
- Make risk-based decisions on what will do the most good.
- Use available frameworks: NIST, CIS, OWASP, COBIT.

Bill

THE "A-LIST"

- Patching
- Secured configurations (workstation/server/applications)
- Password Policy, and consider MFA
- Anti-Virus/Anti-Malware – Still considered baseline
- Infrastructure/Firewall. Web-filtering. Block lists.
- Backups
- Mobile Devices/IOT
- Encryption where applicable
- SIM/SIEM
- Phishing training and testing – KnowBe4, Wombat PhishMe, etc.

Bill

HUMAN & ORGANIZATIONAL CYBER HYGIENE

- It ***IS*** the data, but it is also the people and the organizational environment.
- Where does security fit in the organization?
- Leaders' Backing. Not IT only.
- Create a culture.
- CISO/ISO should champion, but cannot do it alone.
  - Security? IT's got that. They will take care of it.
  - CISO is a champion who markets a very important message.

AI

RISK MANAGEMENT

- All security is risk based. Speak the language.
- It IS about the data.
    - Identify
    - Classify
    - Involve leaders, and departments (Data Owners)
- Develop a Risk Analysis, and a Risk Management Plan.
- Prioritize actions for user-departments, for security and for IT
- Eliminate, mitigate, transfer (Cyber-Insurance), accept
- Consumer-driven technologies.
- Somewhere, we need to balance function and security.

AI

HUMAN & ORGANIZATIONAL CYBER HYGIENE
(CONTINUED)

- Training and Reminders.
- Information Security Policy.
- Training and Reminders.
- Create a culture. Strive for adoption by the organization.
- Incident response planning.

AI

HUMAN & ORGANIZATIONAL CYBER HYGIENE
(CONTINUED)

- You have to convince your leaders.
- Asset Management – cradle to grave.
- Prioritize, Prioritize, Prioritize
- Compliance-related project, such as HIPAA, CJIS, PCI-DSS, etc.
- Training and Reminders. Tip: In your security Emails, include things about family – financial, cyber-bullying, online safety, etc.
- Become the Security Advocate for your organization.

AI

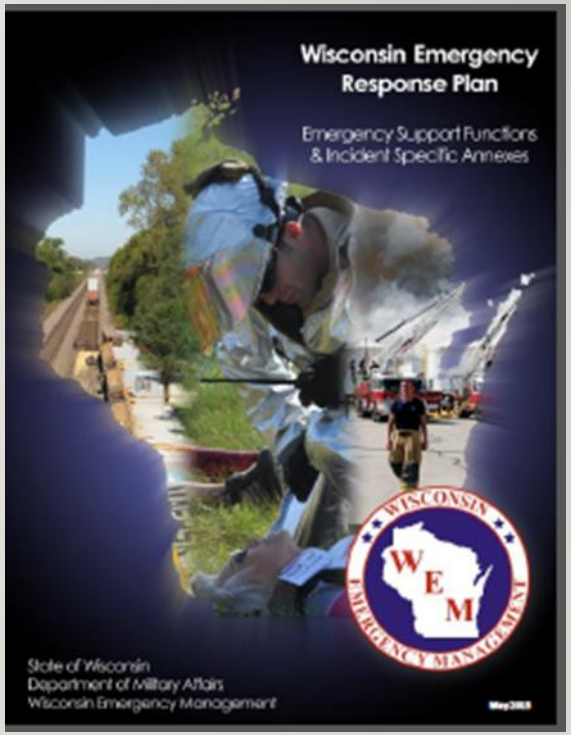
THE CAVALRY
HOW TO GET HELP

- We cannot do this alone.
- Fortunately, a number of organizations offer training, education and assistance. Here are some of them:
  - MS-ISAC
  - SANS.org
  - GIPAW
  - HIPAA-COW
  - Infragard
  - Blogs, like Krebs on Security, Bruce Schneier, and others.
- Colleagues, vendors. Collaborate and share ideas.

Bill

STATE OF WISCONSIN CYBER INCIDENT RESPONSE

- Wisconsin Emergency Response Plan
- Response teams:
  - Government Teams
  - Private Sector Team
  - WI National Guard
- Receive training to assist in a time of emergency.
- Not law enforcement, but provide assistance.



Bill

COMMENTS/QUESTIONS??

- Bill Nash, State of Wisconsin CISO, bill.nash@Wisconsin.gov
- Allen Mundt, Waukesha County ISO, amundt@waukeshacounty.gov

Thank You !!