

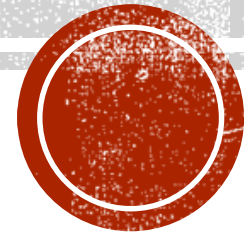
ENHANCING RESILIENCE: CYBERSECURITY AND REGIONAL COORDINATION

A VIEW FROM WISCONSIN

Jeffrey Thomas, CISA, CISM, CISSP-ISSMP

Chief Information Officer

Public Service Commission of Wisconsin



MEET THE NEW THREAT, SAME AS THE OLD THREAT

- Cyber offenders are “lazy.” (When they can be...)
 - Continue to use known, existing, proven methods to gain entry.
 - SQL Injection – 20 year old vulnerability
 - Phishing e-mail – not always a Nigerian Prince
 - Through the unpatched, unhardened (secured/locked down) system on the Internet
 - Exploiting out of date software languages and frameworks
 - Spreading viruses and malware
 - Usable tools are downloadable from the Internet
 - Add-ons targeting specific systems can be added
 - Social engineering
 - Phone calls, or even walking through the front door
 - Nation States continue to set the high bar for sophisticated cyber attacks



MEET THE NEW THREAT, NOT THE SAME AS THE OLD THREAT

- Movement of nation-state talent into the criminal sector.
 - Organized crime is becoming nearly indistinguishable in their sophistication from nation states. (Indistinguishable in the very near future, or some argue indistinguishable now.)
- Cyber Crime is a big and growing business.
 - You can buy a zero day attack package/method on day 0.
 - Cyber attacks as a service is a growing criminal enterprise.
 - Ransomware is a growing method of extorting payment.
- Traditional anti-virus software is less effective every day. (But you still need it.)
 - Current malware and viruses can morph on your system to avoid detection.
 - Code can be executed on your system in memory without writing to disk using normal services, looking to many defensive systems as legitimate traffic.
- PowerShell exploits are old news. (But still important.) Browser features and new operating system functions (including security functions) are increasingly popular for hackers.
- Increased focus on widely used hardware flaws.
 - Computer processor flaws (i.e. Intel)



WHAT IS WISCONSIN DOING?

- Multi-agency/organization initiative underway to create K-Bachelor's Cyber Education curriculum for public schools, technical colleges and state universities
- Wisconsin Cyber Security Planning Work Group
 - Supports initiatives of the Wisconsin Homeland Security Council
 - Comprised of key personnel from critical state agencies as well as utilities and healthcare systems.
- Currently in process of developing a new cyber response plan for cyber events
- Increasing investment in enterprise and agency cyber capabilities
- Annual Governor's Symposium on Cyber Security
- Cyber response being built into numerous emergency response exercises.



WHAT IS WISCONSIN DOING?

- Formed Cyber Response Teams
 - Several teams, including one which is made up of cyber responders from utilities and the PSCoW
 - Other teams comprised of National Guard, State, County and Local cyber professionals
 - Teams train together in cyber skills for normal defense and response operations
 - Teams respond to actual cyber incidents throughout the state
 - Work with law-enforcement as appropriate
- Sharing Intel
 - Wisconsin Cyber Threat Response Alliance (WICTRA)
 - New organization including WI-DOA, WI-DMA, PSCoW and several utilities.
 - Associated with with ACTRA (Arizona Cyber Threat Response Alliance)
 - Working with University of Wisconsin to stand-up a Security Operations Center
 - Will share near-real time de-identified security event information.



WHAT IS WISCONSIN DOING?

- Madison Gas and Electric has built a \$1 million cyber range which is being used for state level exercises.
 - Will be part of next week's Dark Skies exercise
- Public Service Commission of Wisconsin is working with the University of Wisconsin – Whitewater
 - Cyber Security and Risk Assurance class student teams conducted a security audit at the PSCoW for their fall 2018 semester.
 - Included physical security assessment, review of policies and procedures, as well as our computer system defensive posture.
 - Provided PSCoW with additional manpower while students applied classroom knowledge to real world situations.
 - PSCoW provides UW-W students majoring in IT with an emphasis in Cyber Security with Internship opportunities

