2015

3rd Annual

WISCONSIN CYBERSECURITY SUMMIT

AGENDA

Meeting Wisconsin's Cybersecurity Challenges through Public and Private Partnerships

Wednesday, October 28, 2015

8:00 AM - 8:30 AM **Registration**

8:30 AM - 9:00 AM **Opening Keynote: Governance/Planning – Adjutant General Dunbar**

This marks our third year for the Wisconsin Cybersecurity Summit. While we continue to invest in cyber prevention of threats and attacks, they are increasing, and globally driven by motives ranging from criminal theft and social messaging to economic espionage and cyber warfare. Now, we need to match these investments with a focus on response with public and private resources in a collaborative manner.

9:00 AM - 9:30 AM **Wisconsin's Cyber Situational Awareness – David Cagigal – State of WI CIO (2014 NIST Framework)**

David's presentation will focus on: Identify and distinguish between data breach of personally identifiable information (e.g., Social Security and credit card numbers) vs. cyber threats and attacks on our Critical Infrastructure and Key Resources (CIKR). Data breaches are significant and typically referenced in the headlines, but a more serious concern is a cyber disruption in infrastructure that would lead to a domino effect. Therefore, our measure of protection will balance risk mitigation with cost. Further, focusing on our infrastructure, we must detect cyber threats and attacks in a timely manner to respond in a commensurate manner to the threat and/or attack, while understanding the interdependencies of all sectors. If necessary, recovery efforts need to be collaborative and timely.

9:30 AM - 10:00 AM **Detection of Cyber Threats and Attacks – Thomas MacLellan – FireEye, Inc.**

Detection against a cyber threat and/or attack requires substantial investments in people, processes and technologies. We are building State, Local, Tribal and Territory (SLTT) Response Teams as well as well-defined processes that interface with Emergency Management services. There are significant investments in traditional cybersecurity products and services, including a managed security services contract. Likewise, state government is working with the University of Wisconsin to establish monitoring services with cybersecurity students, to encourage development of the profession.

10:00 AM - 10:15 AM **Morning Break**

10:15 AM - 10:45 AM **"Fact vs. Fiction: Critical Infrastructure Cyber Attacks and What You Can Do" – Robert M. Lee, SANS Institute**

There are a number of cyber attacks that have occurred on Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) critical infrastructure sites - but there are also a number of reported attacks that never occurred. This presentation will focus on dispelling some of the hype around the fictional cyber attacks while highlighting the need for defense and lessons learned from the factual attacks. The talk will conclude by highlighting some of the research being done at the SANS Institute for helpful models to protect critical infrastructure.

10:45 AM - 12:00 PM **Panel Discussion: Wisconsin State Agency Cyber Roles Supporting: Identify, Protect, Detect, Respond, and Recover**

Moderator – David Cagigal, Department of Administration
Homeland Security Council Member – Mike Huebsch, Public Service Commission
Energy Sector – William Lucas, We Energies
Secretary, Ray Allen, Department of Financial Institutions
Financial Sector – Brent Maher, Johnson Bank
Homeland Security Council Member – Paul Hammer, Department of Transportation
Transportation Sector – Brian Bobo, Schneider Trucking

This discussion will highlight the cyber incident roles of the agency in the context of its primary sector responsibilities. Introductory remarks by agency representatives:

- Industry (sector) overview.
- Agency mission, goals, metrics.
- Primary federal partners.
- Cyber focus in the industry/sector.

12:00 PM - 1:00 PM **Box Lunch**

Afternoon Demonstration

1:00 PM - 3:15 PM **Alphaville Visual Demonstration**

Come visit Alphaville! This visual cyber range simulates a small town that falls victim to various cyber attacks. The challenging environment develops and evaluates your skills in one or more of the following areas: penetration testing, forensic examination, WEB security, password security, and SQL security.

Breakout Sessions

BREAKOUT SESSION

1:00 PM - 2:00 PM **Enabling an Effective NIST Framework for Secure Citizen Engagement – Vik Bansal and Sam Arias, Deloitte & Touche LLP**

Agencies are increasing their online connections and services to citizens. This new model of citizen engagement requires an enterprise framework to better manage associated risks. Join this session to understand how organizations are taking a strategic approach to managing cyber risks by implementing the NIST framework as part of an enterprise strategy. This strategy includes NIST risk assessments that feature data classification, and cataloguing & mapping the flow of high-risk data elements so the framework is better aligned with the business. Hear lessons learned from states that have enabled this framework, and how building a Secure.Vigilant.Resilient™ strategy that includes new technologies such as continuous monitoring, can better protect citizen information.

BREAKOUT SESSION

1:00 PM - 2:00 PM **Partnering to Protect Wisconsin From Outsider and Insider Cyber Threats – Byron Franz, FBI**

Wisconsin's business secrets and vital systems are under constant attack from Advanced Persistent Threats (APTs), criminals, and even trusted insiders. Using some Wisconsin case examples, this presentation will highlight some these threats, discuss their Techniques, Tactics, and Procedures (TTPs) , and suggest possible mitigations. Emphasis will be how Wisconsin's business, academic, and governmental organizations leverage effective partnerships to identify, protect, detect, and respond to escalating cyber threats.

BREAKOUT SESSION

1:00 PM - 2:00 PM **Panel Discussion: Recruitment of IT Talent**

Moderator - Dr. Joe Adams, Merit Network, Inc.
Bill Nash, CISO, Department of Administration
Bob Turner, CIO, University of Wisconsin
Panel Speaker - TBD

While all cyber strategies and plans focus on processes, technologies and people, there is growing consensus that there is and will be a shortage of talented cyber professionals globally. Both public and private organizations need to address their recruiting, developing and retaining of staff. This is already a very competitive market. The panel will address proven recruiting strategies, training plans and retention activities.

2:00 PM - 2:15 PM **Afternoon Break**

BREAKOUT SESSION

2:15 PM - 3:15 PM **Threat Communications – Chris DeRemer, WSIC and STAC**

When a cyber disruption occurs, we must be ready to respond and execute a well-designed strategy and plan that orchestrates the appropriate private and public organizations – otherwise we will be layering chaos on top of chaos. Further understanding the interdependencies of CIKR sectors (e.g., energy sector impacts all other sectors) requires significant collaboration of communication processes, including the receipt of information, discerning the information, and routing to the appropriate parties in a timely manner. We must also leverage our physical Emergency Management services (resources, structures and processes) when necessary.

BREAKOUT SESSION

2:15 PM - 3:15 PM **Risk Detection – Think Global, Act Local – John D. Velisaris, IBM**

Protecting State of Wisconsin data is of paramount importance every single second of the day. IBM is augmenting cyber security protection resources through a Managed Security Services contract. Our partnership balances cost, complexity and effectiveness in our risk mitigation efforts. Collectively the State of Wisconsin and IBM leverage technologies, processes and people to proactively detect cyber threats and attacks through greater visibility and robust analytics; all in efforts to mitigate risks. John's discussion will focus on the benefit, and the challenge, of leveraging global threat activity to detect and react to local events.

BREAKOUT SESSION

2:15 PM - 3:15 PM **Developing Talent Through Training – Dr. William J. (Joe) Adams, Merit Network, Inc.**

As competitive as the IT job market is, it is crucial for managers to be able to hire and retain the right people. From the job seeker perspective, it is equally important to be prepared and to maintain the skills that managers are looking for. In this talk, Dr. Adams will discuss the role of certifications in the IT industry and present some ideas on how organizations can use a cyclic approach to keeping their workforce's skills up to date and their workers engaged.

Conclusion

3:15 PM - 4:00 PM **Conclusion – Five News You Can Use: Identify, Protect, Detect, Respond, Recover – Major General Donald P. Dunbar**

Adjutant General Dunbar will summarize the 2014 NIST Framework – IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER. Today's sessions have illustrated the importance of our public and private collaboration in preventing and responding to cyber threats and attacks. Our CIKR sectors are interdependent. Our collective efforts to Identify, Protect, Detect, Respond and Recover are the basis for our Cyber Disruption Response Strategy under development.