Meeting 06

November 20, 2024

Attendees

Members – Bold and *Italics* attended

Denise Reilly-Hughes	~~John Toney~~	*Erica Ferland*
~~Joe Duncan~~	~~Nate Couture~~	*Eric Hillmuth*
Eric Forand	*Shawn Loan*	~~Gregory C. Knight~~
James Layman	*Sue Fritz*	*Jason Galipeau on behalf of General Knight*

Invited Guests – Bold and *Italics* attended

~~John Zanin~~	*Michelle Anderson*	*Shawn Nailor, CIO designee*
Jon Kelley	~~AJ Van Tassel~~	~~Hazel Kreider~~
		David Kaiser on behalf of John Toney

Public – None

Agenda

- Review last meeting recap – any corrections or clarifications – ***Complete, no changes***
- Administration - ***Complete***

    - Set meeting schedule for 2025 – *Third Wednesday from 1:30 to 3:00 in January, March, May, July, September, November*
- Review Strategic Plan – *Complete, document markup*
- Review Annual Report – *Next meeting*
- Open discussion - *None*
- Adjourn

Outcomes

Motions

- *Motion to set the 2025 meeting schedule for the third Wednesday of January, March, May, July, September, and November from 1:30 to 3:00. Motion made by Sue Fritz, seconded by Eric Forand. All in favor.*
- *Motion to adjourn by Sue Fritz, seconded by Denise Reilly-Hughes. All in favor.*

Summarize.tech Recap - edited for clarity

- During the final Cybersecurity Advisory Council meeting of 2024, members reviewed previous discussions, set a meeting schedule for 2025, and worked on the draft of the Strategic Plan and annual report.
- The council confirmed they will meet on the third Wednesday of odd months in 2025, with a focus on refining the insights from earlier discussions to enhance the Strategic Plan.
- They explored presenting cybersecurity survey data in a clear manner, contemplating different visual formats and emphasizing the importance of accuracy in depicting organizational preparedness. The conversation also highlighted the need to differentiate between "I don't know" and "no" responses in surveys and the significance of tailoring cybersecurity strategies to diverse sectors.
- Goals were established to enhance awareness and readiness for critical infrastructure operators, while participants reviewed the alignment of their objectives with measurable outcomes, recognizing the need for clarity on funding and organizational involvement to ensure successful implementation of initiatives.
- Participants discussed the importance of piloting tier one services before wider rollout, emphasizing flexibility and the need for ongoing evaluation to assess program effectiveness.

- Future initiatives for 2025 were outlined, including outreach to critical infrastructure operators, partnerships with local educational institutions, and non-profits like the Cyber Readiness Institute, and enhanced incident response capabilities inspired by models like Wisconsin's cyber initiative. A tiered support strategy for organizations was proposed, promoting a clear framework for education and collaboration.
- The meeting concluded with discussions on pilot testing based on hospitals, aiming for diverse representation, and the chair urged members to provide feedback on the strategic plan, with the goal of refining it for legislative review in January.