Trustworthy CPS and Educational Initiatives

Discussion Summary

Rick Schlichting

Overall, the discussion covered challenges in interdisciplinary appointments, strategies for tenure cases, the importance of broad cybersecurity education, industry demands, liability issues, and the role of government initiatives in shaping cybersecurity education

1. **Challenges of Interdisciplinary Appointments for Junior Faculty:**
   - Joint appointments can be challenging for junior faculty, especially in tenure cases.
   - Difficulty in obtaining letters and dealing with different academic standards.

2. **Addressing Interdisciplinary Challenges:**
   - Hiring individuals at the intersection of disciplines who believe in the future of multidisciplinary communities.
   - Creating a deliberate and safe space for faculty with joint appointments.
   - Providing clear expectations through a two-page memo outlining tenure expectations.

3. **Diversity in Academic Standards:**
   - Highlighted differences in academic standards between computer science and public policy.
   - Emphasized the importance of understanding and respecting diverse academic models.

4. **Navigating Interdisciplinary Tenure Cases:**
   - Developing strategies for evaluating faculty success in interdisciplinary settings.
   - Signaling to letter writers the importance of recognizing contributions in both disciplines.

5. **Structural Challenges in Academic Departments:**

   - Importance of structuring joint appointments to address workload and retirement considerations.

   - Aligning tenure home with the department that values interdisciplinary contributions.

6. **Mentoring and Shared Experiences:**

   - Acknowledging the challenges of finding shared experiences in interdisciplinary mentoring.

   - Emphasizing the need for community support and mentoring in interdisciplinary fields.

7. **Undergraduate Cybersecurity Education:**

   - Discussing the flexibility in undergraduate cybersecurity education.

   - Allowing students to choose trajectories that align with their interests, whether technical or social science-oriented.

8. **Philosophical Approach to Cybersecurity Education:**
   - Debating the best approach to cybersecurity education.
   - Discussing the possibility of integrating basic security knowledge into all disciplines.

9. **Incorporating Security Competency:**
   - Proposing the integration of security competency into various courses.
   - Suggesting a competency-based approach to cybersecurity education.

10. **Ensuring Broad Security Knowledge:**
    - Emphasizing the importance of ensuring all students have basic security knowledge.
    - Considering the impact of technology development without incorporating security at the beginning.

11. **Addressing Industry Needs:**

- Recognizing the need for cybersecurity professionals with a background in safety and industrial systems.
- Discussing industry demand for professionals with competencies in both cybersecurity and safety engineering

12. **Liability and Responsibility in Software Development:**

- Highlighting the need for liability and responsibility in software development.
- Discussing the importance of standards and best practices to reduce risks and enhance security.

13. **Professional Degree Programs:**

- Identifying the role of professional degree programs in retraining individuals for cybersecurity roles.
- Recognizing the uniqueness and challenges of professional master's degree programs.

14. **Government Initiatives and Cybersecurity Strategy:**

- Acknowledging government initiatives in cybersecurity education.
- Discussing the national cybersecurity strategy and the role of education in reducing risks.

15. **Incentivizing Responsible Computing:**

    - Proposing the idea of incentivizing responsible computing through liability and consequences.

    - Discussing the importance of reducing demand for insecure systems.

16. **Challenges in Security Labeling:**

    - Expressing concerns about the government's approach to security labeling.

    - Differentiating between knowing the contents of a box and proving its security.

17. **Open Source Software and Security:**

    - Recognizing the differences between closed-source and open-source software in terms of security accountability.

And now the secret…..

- Summary generated by ChatGPT 3.5 from audio transcript captured by Whisper*

*Thanks to Assoc. Prof. Margaret Schlichting in the Psychology Dept at the University of Toronto for suggesting the use of ChatGPT.