1. Your upcoming presentation at the ISACA Risk Event is titled *“The Double-Edged Sword: Risks of AI Language Models in Cybersecurity.”* What inspired you to focus on this topic, and why is it critical for cybersecurity professionals to understand these risks now?

I tailored this presentation specifically for the ISACA Risk Event audience, focusing on the critical balance between the risks and opportunities of new technologies like AI generative models. These technologies, while offering immense potential, also introduce significant risks that cybersecurity professionals must understand and address. My goal is to emphasize that we cannot allow these risks to overshadow the transformative opportunities AI brings to the field. Instead, we must learn to manage them effectively to unlock AI’s full potential in enhancing cybersecurity.

1. AI tools like GPT-4 have the potential to enhance cybersecurity defenses, but you highlight how they can also be exploited by attackers. Can you share a real-world example where AI was weaponized in a cyberattack, and how should organizations prepare for such threats?

I will be covering several examples in my presentation, both theoretical and actual cyberattacks. Among the most common are phishing and business email compromise (BEC), which attackers can enhance using AI. A particularly interesting real-world case occurred in 2019, when a CEO fraud attack used deepfake audio (vishing) to impersonate a CEO and trick a U.K.-based energy company into transferring $243,000 to cybercriminals. To prevent such incidents, organizations should focus on employee training, raising awareness about AI-enabled threats like deepfakes, and ensuring strict verification procedures are followed before authorizing financial transactions or sensitive actions.

1. Ethical concerns, such as bias and privacy breaches, are often mentioned in the context of AI. In your experience, how can organizations balance leveraging AI’s capabilities while ensuring ethical responsibility and data protection?

Organizations can balance leveraging AI’s capabilities with ethical responsibility and data protection by implementing a few key strategies. First, they should prioritize transparent AI development, ensuring that systems are explainable and that decision-making processes can be audited to identify and address potential biases. Second, they need to enforce data minimization and anonymization practices to protect privacy, ensuring that only the necessary data is collected and stored securely. Third, incorporating fairness assessments and diverse datasets into AI training can help reduce bias. Finally, establishing ethical oversight committees and adhering to regulations like GDPR and EU AI Act ensures that AI innovations are deployed responsibly while maintaining trust and protecting users’ rights.

1. Your presentation also touches on the operational risks of over-reliance on AI in cybersecurity. What practical steps can businesses take to prevent becoming too dependent on AI, and how can they complement AI solutions with human expertise?

To avoid over-reliance on AI in cybersecurity, businesses should adopt a human-in-the-loop approach, ensuring that human expertise remains central to decision-making processes. While AI can efficiently handle repetitive tasks and detect anomalies at scale, humans are essential for interpreting nuanced threats, verifying critical alerts, and making judgment calls in ambiguous situations. Practical steps include providing continuous training for cybersecurity teams to keep up with AI advancements and establishing protocols where humans validate high-risk decisions flagged by AI systems. Additionally, organizations should foster a culture of collaborative cybersecurity, where human analysts regularly review AI-driven insights, adjust algorithms, and maintain oversight to ensure the system remains effective and unbiased. By combining AI’s speed and automation with human intuition and contextual understanding, businesses can build a more resilient and adaptive cybersecurity posture.

1. You wear multiple hats as a principal researcher at Northwave Cybersecurity and an assistant professor at the University of Twente. How do your roles in academia and industry influence your approach to addressing AI risks, and what unique insights can attendees expect from your presentation at the ISACARisk Event?

My dual roles as a principal researcher at Northwave Cybersecurity and an assistant professor at the University of Twente provide a unique perspective on AI risks in cybersecurity. From academia, I approach these challenges with a research-driven mindset, focusing on theoretical advancements, long-term impacts, and exploring emerging risks that may not yet be fully understood in the industry. On the other hand, my industry role grounds me in practical, real-world challenges, where the urgency of mitigating AI risks and protecting against sophisticated attacks takes center stage. This combination allows me to address AI risks holistically, balancing cutting-edge research with actionable strategies.

At the ISACA Risk Event, attendees can expect insights that blend academic rigor with industry pragmatism. I’ll provide a forward-looking view on AI risks, while also offering concrete, practical steps for organizations to mitigate these threats today. This approach ensures that businesses can leverage AI effectively while staying ahead of the rapidly evolving threat landscape.