Insights on the Current State and Future of Cybersecurity

with Dr. Faisal Kaleem

PROFESSOR AT METRO STATE UNIVERSITY

Dr. Faisal Kaleem, Computer Science & Cybersecurity Professor

Dr. Faisal Kaleem is a Professor in the Department of Computer Science and Cybersecurity at Metro State University. He earned his PhD in Electrical Engineering from Florida International University, Miami, FL, and has been a committed educator since 1998. An award-winning cybersecurity educator, he has made significant contributions to the field both nationally and within Minnesota, particularly in fostering a diverse cybersecurity workforce and establishing a comprehensive cybersecurity ecosystem. His research uses Augmented Reality (AR) to explore the characteristics of cybersecurity learners and address AR's privacy concerns, enhancing his broader focus on developing cybersecurity and forensic curricula. Dr. Kaleem's work is supported by substantial grants from the NSF, NSA, and various state and private entities. Holding esteemed industry certifications such as CISSP, Dr. Kaleem is also celebrated for his commitment to teaching, evidenced by multiple awards for excellence in teaching and accolades from the professional community.

We asked Dr. Kaleem to share some insights on the current state of cybersecurity, its impact on government and private industry, and what the future of cybersecurity may bring. His valuable insights follow:

Could you briefly share your journey in the cybersecurity field and what inspired you to focus on this area?

My journey into cybersecurity was not straightforward, beginning with a Bachelor's degree in Electrical Engineering and evolving through various pivotal experiences. Initially focused on engineering, my curiosity led me to reverse-engineer toys and eventually write a TSR keylogger program, igniting my interest in cybersecurity. My Master's thesis on Steganography further deepened this interest. Transitioning into academia, I developed an information security course and and contributed to an online cybersecurity master's program. Since joining Metro State University in 2014, I have worked to elevate its cybersecurity curriculum, driven by a passion for advancing the field and nurturing future cyber professionals.

What are the most significant changes in cybersecurity over the past decade?

Over the past decade, significant changes in cybersecurity include the rise of sophisticated cyber threats like ransomware and state-sponsored attacks, the increased importance of cloud security due to widespread cloud adoption, advancements in AI and machine learning for threat detection and response, the growing focus on zero-trust security models, and enhanced regulatory frameworks like GDPR and CCPA to protect data privacy.

> Additionally, the proliferation of IoT devices has introduced **new vulnerabilities, necessitating more robust security** measures across diverse environments.

The advent of AI would seem to set up situations where both the perpetrators and the defenders will use AI in the cybersecurity realm. If so, where do humans fit in?

In the cybersecurity realm, even as both perpetrators and defenders increasingly leverage AI, humans remain crucial. Human expertise is essential for developing, training, and fine-tuning AI algorithms, ensuring ethical use, and interpreting AI-generated insights. Additionally, humans are needed to make strategic decisions, handle complex threat analysis that AI might miss, and respond to sophisticated social engineering attacks.

> Ultimately, **human intelligence and creativity are vital** for adapting to evolving threats and innovating new defense strategies.

What do you believe are the most significant differences in the cybersecurity needs of government and the private sector?

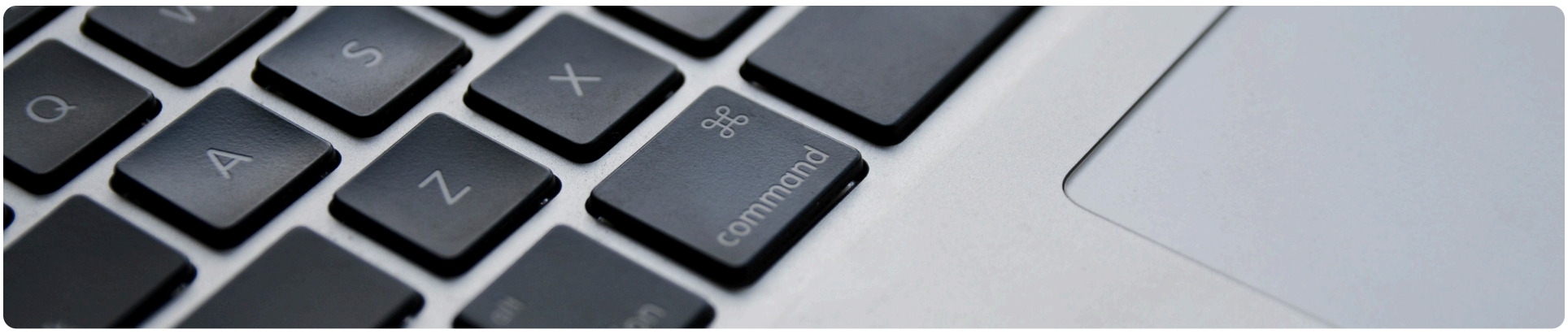
The most significant differences in the cybersecurity needs of government and the private sector lie in their focus and scale of threats. Government cybersecurity often prioritizes national security, protecting critical infrastructure, and addressing state-sponsored cyber threats, requiring stringent protocols and advanced defense mechanisms. In contrast, the private sector focuses on protecting intellectual property, customer data, and financial assets, balancing security with business operations and compliance with industry-specific regulations. While both sectors face common challenges, the scope, scale, and nature of their threats and priorities differ significantly.

You and your students worked with Inkit on a research project involving cybersecurity in the secure document generation (SDG) space. Were there any learnings on that project that stuck out to you?

Metro State students provided pen-testing services on the SDG platform. This hands-on penetration testing project offered significant benefits to students by providing practical, real-world experience in cybersecurity. It allowed them to apply theoretical knowledge to a real-world environment, enhancing their problem-solving and critical-thinking skills. Engaging in this project helped students understand the methodologies and tools used by attackers, which, in turn, sharpened their defensive strategies. This immersive learning approach boosted their confidence and competence in identifying and mitigating vulnerabilities, making them more adept at handling actual cyber threats.

What critical applications require extensive cybersecurity efforts that the public doesn’t realize the importance of?

Critical applications requiring extensive cybersecurity efforts that the public often overlooks include medical devices and healthcare systems, industrial control systems (ICS) for utilities and manufacturing, financial systems and banking infrastructure, and the supply chain and logistics networks. These applications are vital to daily life and national security, and their disruption could have severe consequences, highlighting the need for robust cybersecurity measures.



It would seem very important that cybersecurity curricula include an emphasis on ethics. Is this a part of your program?

Yes, our cybersecurity program includes a strong emphasis on ethics. We believe it is crucial for students to understand the ethical implications of their work, ensuring they can make responsible decisions in protecting data and networks. Our curriculum covers topics such as ethical hacking, privacy concerns, and the legal aspects of cybersecurity. By integrating ethics into our courses, we prepare students to navigate complex moral dilemmas and uphold the highest standards of professional integrity in their careers.

Your organization MN Cyber teaches that indiviual and team skills are critical components of effective cybersecurity in addition to effective use of digital tools. How is this manifested?

In our cybersecurity program, individual and team skills are developed through hands-on labs, group projects, and real-world simulations. Students work both independently and collaboratively to solve complex security challenges, enhancing their technical expertise and teamwork capabilities. This approach ensures they are proficient with digital tools and can effectively communicate, coordinate, and strategize within diverse teams.

What threat types that aren't well known now may become very dangerous in the near future?

Emerging threats that may become very dangerous in the near future include AI-driven attacks, deepfake technology, quantum computing vulnerabilities, and advanced IoT device exploits.

> As these technologies evolve, they could be **leveraged to create more sophisticated and harder-to-detect cyber threats**, posing significant risks to security infrastructure.

Additionally, threats targeting supply chains and critical infrastructure could become more prevalent as attackers seek to exploit interconnected systems and the increasing complexity of global networks. Proactive measures and continuous research are essential to stay ahead of these evolving dangers.

Move Missions Forward.

(888) 899-7773 | sales@inkit.com | www.inkit.com