May 2025 Isssue 02

THE CENTER FOR DATA ANALYTICS AND CYBERSECURITY (CDAC) NEWSLETTER

Welcome to the second issue of the CDAC Quarterly Newsletter. As we move through 2025, the Center for Data Analytics and Cybersecurity (CDAC) continues to expand our reach, deepen partnerships, and strengthen the region's capabilities in cybersecurity and data science. This past quarter has been especially exciting, and we're proud to share several key milestones that reflect our growth and impact.

A major highlight was hosting cybersecurity training in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA). Professionals from across CISA Region 6 gathered at this event to explore contemporary threats and practical defense strategies. The local delivery of Nation Lab instruction further contributed to building regional cybersecurity resilience.

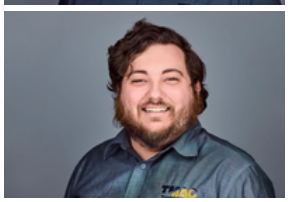
We are also pleased to announce the approval and upcoming launch of a new Graduate Certificate in Enterprise Cybersecurity at Lamar University. This program will serve as a valuable opportunity for professionals seeking to enhance their knowledge in cybersecurity and enterprise-level risk management. More details on page 3.

Finally, we completed the design of our Cyber Testbed Demonstration Unit, which will allow hands-on demonstrations of real-world cyberattacks and defense techniques. This mobile unit will support education, outreach, and public engagement in a way that brings cybersecurity to life. Thank you for supporting CDAC's mission. We look forward to continuing this important work together.

Helen Lou
Director
helen.lou@lamar.edu

Adam Loucks
Program Manager
aloucks@lamar.edu

Joseph Raymer
Cyber Research Scientist
jraymer1@lamar.edu



LAMAR UNIVERSITY HOSTS REGIONAL CYBERSECURITY TRAINING WITH CISA AND INL

From April 15–18, Lamar University hosted the CISA Region 6 Industrial Control Systems (ICS) Cybersecurity Training Workshop in partnership with Idaho National Laboratory (INL). This live training was provided specifically for members of the industrial control systems community associated with IT and process control network operations and security (Operations Technology, OT), operations or management of critical infrastructure (CI) assets and facilities, as well as those who provide CI components and software development. This four-day, hands-on event brought together professionals from energy, utilities, manufacturing, municipalities and the Coast Guard to enhance cybersecurity preparedness across critical infrastructure sectors.

INL instructors led technical sessions, including Introduction to Control Systems Cybersecurity (101), Intermediate ICS Cybersecurity (201 & 202), and CyberStrike: Lights Out—a live simulation of defending against an OT cyberattack. Attendees included representatives from ExxonMobil, Shell, Motiva, BASF, Cheniere Energy, Entergy, and many others.

CISA Region 6 covers Texas, Louisiana, Arkansas, Oklahoma, and New Mexico. This workshop strengthens cybersecurity awareness and capabilities within the industrial control systems sector in CISA Region 6. It also supports regional workforce development and fosters collaboration among industry, government, and academia. Given the strong attendance and positive feedback, there is clear momentum to make this a recurring event

The event featured remarks from U.S. Representative Randy Weber and George W. Reeves from CISA Region 6, both highlighting the importance of infrastructure protection and workforce development. The workshop was supported by two DOE grants, “Southeast Texas Data Analytics and Cybersecurity for Energy Supply Chain Resilience” (DE-CR0000035) and “Midstream Critical Manufacturing Industry Cybersecurity Hub” (DE-CR0000037).

GRADUATE CERTIFICATE IN ENTERPRISE CYBERSECURITY

18 Credit Hours | 6 Courses | Launches Fall 2025 | Available Online and On-Campus | STEM-Designated

The Graduate Certificate in Enterprise Cybersecurity at Lamar University is a flexible, fast-track program designed for working professionals and graduate students seeking advanced training in cybersecurity. The certificate consists of 18 credit hours (6 courses) and can be completed in as little as 24 weeks, with courses delivered in accelerated 8-week sessions. Starting in Fall 2025 (August), the program is offered fully online or on-campus, making it ideal for both full-time students and working professionals.

The curriculum is structured around three key domains—Foundational Concepts, Technical Core, and Non-Technical Core—to ensure well-rounded, practical knowledge. Students will complete at least two courses from each domain, covering topics such as cybersecurity principles, scripting, network defense, risk analysis, policy, and management.

This certificate is ideal for those who want to:

- **Upskill for roles in cybersecurity or IT leadership**
- **Lay the groundwork for further graduate study**
- **Transition into cybersecurity from an allied discipline**

Entry Requirements:

- **A bachelor's degree from an accredited institution in an allied field**
- **Minimum undergraduate GPA of 2.5**

Cost & Registration:

- **Apply through GoApplyTexas.org**

For more information, visit the Lamar University Catalog, or contact the College of Business or the College of Computer Science.

If you have any questions or need any further clarification, please reach out to:

Kakoli Bandyopadhyay, Ph.D.
Chair and Professor of MIS
Department of Information Systems
College of Business
Lamar University
Beaumont, Texas 77710
email: k.b@lamar.edu
phone: 409 880 8627

“PROBABILITY AND TRUTH, THE NOW AND FOREVER LANDSCAPE”

On April 24th, Lamar University hosted an insightful talk titled “Probability and Truth – The Now and Forever Landscape,” featuring industrial cybersecurity expert Marco (Marc) Ayala. The event brought together professionals across critical infrastructure sectors to explore the growing cybersecurity challenges posed by increasingly connected automation systems.

Marco Ayala shared his extensive knowledge on practical strategies to secure industrial control systems, emphasizing the Consequence-Driven, Cyber-Informed Engineering (CCE) approach. Drawing from recent cyber incidents and decades of experience, he highlighted how industries can apply cybersecurity standards, such as ISA/IEC 62443, to build safer and more resilient operational technologies.

As InfraGard Houston President and U.S. Coast Guard Area Maritime Security Committee Cyber Chair for the Gulf of America, Marco offered unique insights from both government and industry perspectives. Attendees left better equipped to understand and address the evolving cyber threats facing energy, manufacturing, water, and transportation sectors.

The session reinforced Lamar University’s commitment to advancing cybersecurity awareness and workforce development in the region.

INFRAGARD
MEMBERS ALLIANCE
HOUSTON