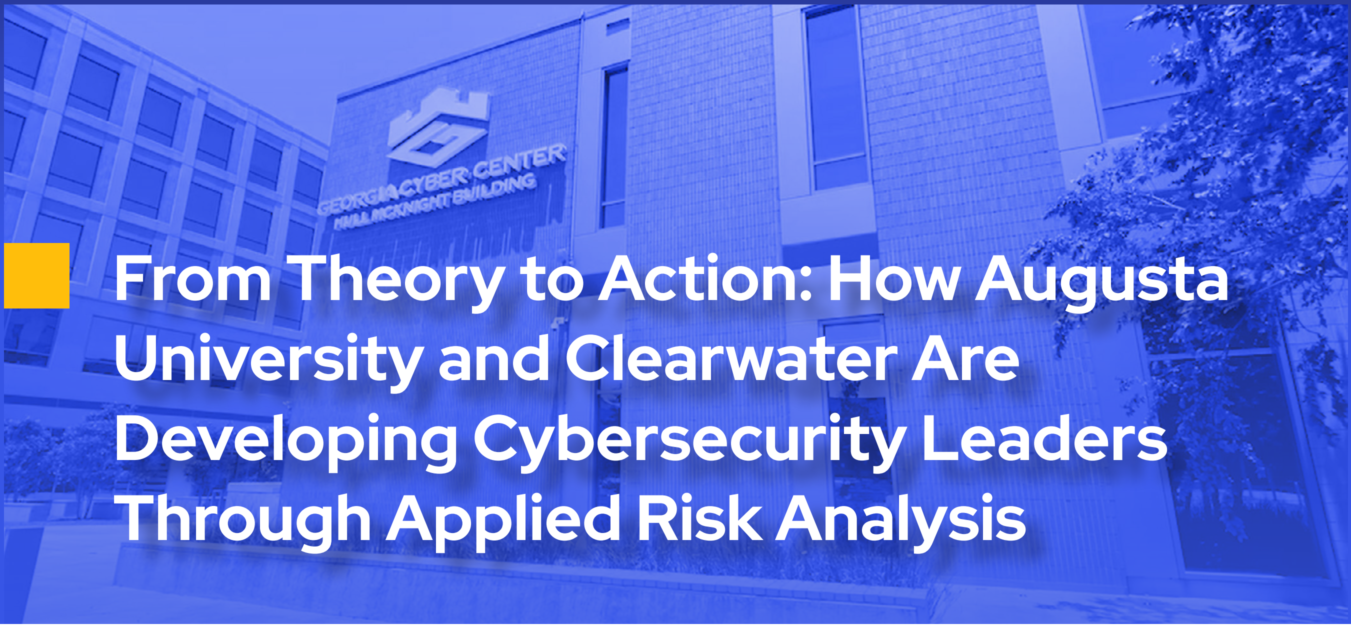
Clearwater Client Success Story | Augusta University



From Theory to Action: How Augusta University and Clearwater Are Developing Cybersecurity Leaders Through Applied Risk Analysis

Most cybersecurity programs prepare students for theory.

At Augusta University (AU) Cyber Defense, students enter a fully operational cybersecurity program, known as SIEGE CyberOps, where they train for what many professionals call the real frontlines of cybersecurity.

Officially branded as Security Intelligence and Engineering for Georgia Education (SIEGE) CyberOps, Augusta Cyber Defense space serves as the home of the university's cybersecurity team and a critical learning environment for students and military interns. Its mission is clear: Protect AU data and networks. Defend against active cyber threats. Educate the workforce through cybersecurity awareness and hands-on experience.

SIEGE CyberOps is structured around three key disciplines: Governance, Risk, and Compliance (GRC); Cybersecurity Engineering; and Security Operations. This comprehensive approach ensures that students, military veterans, and transitioning professionals gain not only technical expertise but also experience working with real-world governance frameworks and risk management strategies.

Step inside the Cyber Defense Department on any given Tuesday, and you won't find students buried in textbooks. You'll find them shoulder-to-shoulder with AU Cybersecurity professionals and military professionals in career transition, eyes locked on live threat dashboards, analyzing vulnerabilities, and making decisions that matter.

The Challenge: Turning Theory Into Readiness

Cybersecurity education has long struggled to keep pace with a rapidly evolving threat landscape. The industry constantly cites a talent shortage, yet job seekers often struggle to secure roles due to lack of experience with many if not all job postings requiring 3-5 years of on-the-job experience. Nowhere is this tension more prevalent than in healthcare, where these unique environments demand relevant experience and strategic thinking from day one.

Graduates out of most cybersecurity higher education programs come away simply with theoretical knowledge, leaving them without the practical skills that resource-strapped employers need immediately. Augusta University set out to change that.

> "They may not have five years of experience, but they have a solid one-year deep dive into risk management, engineering, or incident response," said Tiffany Mack, Director of Solutions for AU's Cyber Defense Department.

Through SIEGE CyberOps, AU created an immersive environment where students, SkillBridge military interns, and transitioning professionals contribute directly to protecting AU networks, which includes AU Research, Dental College of Georgia, and Medical College of Georgia.

Powering the theory and application behind their governance, risk, and compliance strategies is Clearwater's IRM|Analysis® software. Designed specifically for the healthcare sector and used by hundreds of hospitals, health systems, physician groups, health plans, and digital health companies to power effective cyber risk management,

IRM|Analysis streamlines complex risk management processes- helping organizations (and in this case, future cyber leaders) identify, assess, and prioritize risks based on both regulatory requirements and business impact and drive an efficient risk remediation process. Augusta University also relies on IRM|Analysis for its own enterprise risk analyses. Because the university's cybersecurity team depends on the platform to manage AU's risks, it was a natural decision to extend that same technology into the classroom, ensuring students are trained on the very tools driving AU's security posture.

This real-world exposure equips students with the same tools and methodologies trusted by leading health systems nationwide, while preparing them to confidently step into high-demand roles.

Clearwater's IRM|Analysis® Software

Empowering the next generation of cyber leaders with:

- **Healthcare-Specific Risk Management:** Built to align with the NIST CSF, HIPAA,, and the Office for Civil Rights' 9 Elements of Risk Analysis.
- **Asset-Level Risk Visibility:** Identify where critical data resides and how it's exposed—enabling smarter, faster decisions.
- **Business-Aligned Risk Prioritization:** Focus on what matters most by mapping security risks directly to business impact.
- **Hands-On Experience with Industry Tools:** Trusted by leading health systems and now by future cybersecurity leaders at Augusta University.

IRM|Analysis® transforms theoretical concepts into actionable skills ultimately preparing students to lead in today's complex healthcare environments.

The Solution: Turning Learning Into Leadership

From day one, students take on defined roles across SIEGE CyberOps' three focus areas. They conduct risk assessments, draft executive reports, and present findings to university leadership, while developing technical expertise plus the critical thinking and communication skills that employers seek for the jobs now in demand.

Utilizing the live IRM|Analysis environment, this is not a theoretical exercise. It's a thorough, asset-level risk analysis starting with identifying where assets reside, understanding what systems interact with PHI, and determining how to prioritize risks based on severity and business impact. The team works with a broad spectrum of sensitive data risks—including those involving PHI, FERPA, GLBA, and PCI—giving students and interns valuable hands-on experience in managing data protection and understanding the compliance requirements associated with each.

> "You can't protect everything," Mack explained. "What we teach them is how to prioritize—how to think like risk managers. That's what makes them stand out in an interview."

Inside the live Security Operations Center, students also take on critical roles supporting active defense operations. They monitor vulnerabilities, respond to security events, maintain a working risk register, and produce reports that inform executive risk decisions. A true reflection of the environments they will enter in the workforce.

Career Outcomes at a Glance

- **83%** of AU Cyber Defense Students enter cybersecurity roles upon graduation.
- **95%** of SkillBridge interns transition directly into the field.
- Graduates have secured positions at top organizations, including **NASA, the NSA, Deloitte, Deutsche Bank**, and leading healthcare systems.

From Classroom Concepts to Practical Application

This multifaceted experience leads to measurable outcomes. 83% of AU students and 95% percent of SkillBridge interns transition directly into cybersecurity roles after completing the program. Graduates have gone on to work at NASA, the NSA, Deloitte, Deutsche Bank, and major healthcare systems.

For many students and interns, SIEGE CyberOps provides their first direct experience with the governance and compliance structures that define leadership roles in cybersecurity.

One former Army SkillBridge intern, highly experienced in technical operations but new to risk management, now leads Governance, Risk, and Compliance efforts at Augusta University. Another graduate used her time on AU's GRC team to develop the skills she now applies as an Audit Analyst at Deutsche Bank.

These aren't isolated outcomes. They reflect a program built to bridge the gap between academic knowledge and operational leadership.

That success has drawn national recognition. Over the past year, more than 345 leaders—from federal agencies to major technology companies—have toured Augusta University's Cyber Defense Department to see the program firsthand. Most recently, the program was honored with the prestigious

CSO50 Award for its innovative integration of students and military personnel into its cybersecurity mission.

> “When industry and government leaders visit and see our students working with IRM|Analysis, it changes the conversation,” Mack said. “They see that we’re not just preparing students for jobs—we’re preparing them to lead.”

Augusta University’s model demonstrates what’s possible when education moves beyond theory into applied leadership and real-world readiness.

> *Clearwater is proud to power this mission—equipping future cyber leaders with the tools, frameworks, and critical thinking skills they’ll rely on to protect the healthcare organizations of tomorrow. Through hands-on experience with our proven risk analysis methodology and software, students learn to make informed, risk-based decisions that align cybersecurity priorities with business objectives—a skill set in high demand across the healthcare industry. Together, we’re building a stronger, more resilient cybersecurity workforce.*

About Augusta University

Located in the historic city of Augusta and across regional campuses throughout the state, Augusta University stands as Georgia’s premier public health sciences and medical research university. It is home to the state’s flagship medical school, the Medical College of Georgia; Georgia’s only dental school, the Dental College of Georgia; and the Georgia Cyber Innovation and Training Center.

About Clearwater

Clearwater helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can achieve their missions. The company provides a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, managed cloud services, and a 24/7 Security Operations Center with managed threat detection and response capabilities.

Learn More

Whether you need help with risk analysis, responding to OCR, or a comprehensive approach to your cybersecurity and compliance program, we can help.