NEWSLETTER

MIC NEWS

JUNE 2026

WELCOME

New Board Members

MEMBER SPOTLIGHT:

ADEMOLA OLANREWAJU

ADEMOLA OLANREWAJU

Tell us about yourself.

I've been fascinated by technology since I was a kid, learning C++ and squeezing every last byte onto floppy disks back when a 2MB anime clip took three days to download. That curiosity never left me. Professionally, though, I took the scenic route: years in sales and territory management, then 15+ years in project management leading strategic, multimillion-dollar initiatives across industries. Somewhere along the way I realized the part I loved wasn't selling, it was solving complex problems. So I went all in on security. I'm now pursuing my M.Sc. in Cybersecurity, hold Security+, the Google Cybersecurity certificate, and PMP, and I'm working hands-on as a SOC I Cyber Project Lead apprentice with my sights set on GRC. Currently working in a space that incorporates use of agentic AI with heavy emphasis on cyber security.

What sparked that early interest in technology?

It was the constraint, honestly. When resources were scarce, every byte mattered, and that turned ordinary computing into a puzzle. Working out binary calculations for fun, fitting a file onto a floppy with no room to spare, salvaging a dying hard drive, those weren't chores to me, they were victories. I think I fell in love with the problem-solving long before I had a word for it. That same instinct, figuring out how systems work and how to make them work better, is exactly what pulls me toward cybersecurity now.

How does your business background help you approach security and GRC differently?

I came up on the side of the business that has to say "yes," sell, deliver, and keep the client happy. So I don't see security as the team that says "no." I see it as a solution provider with a security baseline underneath everything. That reframing matters in GRC, because controls only work if the business actually adopts them. Coming from sales and project management, I know how to translate risk into language leadership cares about and design controls people will follow rather than resent. My goal is to make security something a business wants, not something it's forced to tolerate.

How has your hands-on experience with the MiC Talent Solutions community supported your transition?

It's given me the thing certifications can't, real reps in a real environment with people invested in my growth. MiC has been a turning point in more ways than one. It's helped me identify the transferable soft skills I already carried over from sales and project management, and it showed me I'm not alone on this journey. Cybersecurity is a whole world of coding, policy writing, and building blocks that go well beyond what most people realize, and MiC gave me the platform to grow into it. Working hands-on with NIST and ISO 27001, threat detection, SIEM tooling, and GRC has let me connect the frameworks I study to actual practice. Just as important, I found my tribe: a place to learn from tenured professionals, mentors, and colleagues who are invested in my growth and who normalize the learning curve for someone making this transition. From Ms Mary holding weekend classes to go through cybersecurity textbooks from cover to cover , and MIC builder's course opening door to learn from tenured professionals.

Is there a recent "win" you're particularly proud of?

IWhat I'm proud of right now is less a single trophy and more the proof that the pivot is working: applying frameworks like NIST and ISO 27001 to live problems and watching my project management instincts translate cleanly into security work. Bridging GRC concepts with the operational side, and being trusted to lead on it as an apprentice, tells me the foundation I've built is holding. And true to "win or learn," the moments that didn't go perfectly taught me just as much as the ones that did. Being able to discuss my experience at MiC conference 2026.

What was the turning point that made you pivot to cybersecurity?

There wasn't one dramatic moment so much as a pattern I couldn't ignore. Across all those projects, the work that lit me up was the risk assessments, the compliance audits, the process optimization, the parts where I was protecting something and untangling complexity. I kept gravitating toward the security questions in every initiative. Eventually I had to be honest with myself: the thing I treated as a side interest was actually the work I wanted to do full-time. So I stopped treating it as a hobby and committed to it as a career.

What advice do you have for career-switchers intimidated by the technical side?

You already bring more than you think. The technical skills are learnable, that's the easy part to fix. What's hard to teach is judgment, communication, and the ability to earn trust, and a career-switcher often arrives with those already. So lead with what you have and stay coachable on the rest. I'd rather ask the question than fake the answer, and that mindset has carried me further than pretending ever could. Adopt a "win or learn" attitude and the technical side stops being a wall and becomes a series of puzzles.

Any fun facts, hobbies, or a "manifestation" you're working toward?

I'm genuinely enjoying the learning process right now. I'm not a pro at coding, and AI has made that space a lot more approachable, but more than the tools, I'm training myself to be more aware, to spot lapses in security around me and become a real security advocate. I love taking in the macro ecosystem of the cybersecurity landscape and seeing how all the pieces fit together. I also enjoy immersing myself in different cultures and find real satisfaction in helping people, which is probably why GRC fits me so well. As for what I'm manifesting: I want to grow within the GRC space and help shape the future of the cybersecurity landscape, building security that businesses actually want. Because my best is never second best, and "good enough" never really is.

THE GLASSWING ERA: A WARNING THAT CAME TRUE, AND THE WORK IT LEAVES US

For three years, I warned that we were adopting AI faster than we could govern it. Then a model called Mythos proved the point, and a project called Glasswing showed us the work ahead.

BY IESHEA HOLLINS

The Warning No One Wanted to Hear

IESHEA HOLLINS

For the past few years, I have been warning about, training on, and developing what I call The Art of AI Adoption. Some of you may even remember me speaking on it at last year's MiC Conference. The message was simple, even if it was not always easy to hear.

Organizations were adding AI into their environments faster than they were governing it. Business teams were experimenting, employees were testing tools, and leaders were excited about speed, convenience, and innovation. But in too many places, no one had called the security team into the room. AI was being bolted onto the tech stack because it made life easier. It helped write, summarize, automate, analyze, and respond. It made organizations feel modern and teams feel productive. And because it made life easier, people stopped asking the harder questions.

What data is this tool touching? Who approved its use? What is it connected to, what can it remember, and what can it expose? Who is responsible if it leaks the wrong information or creates a compliance gap no one sees until it is too late?

My warning was that we had quietly created a new kind of exposure. Not a man in the middle, but a non-human in the loop. An insider we trained, trusted, connected to our data, placed near our customers, and never properly supervised.

At the time, that warning was often met with polite nods. People understood the concern, but the urgency had not fully landed. AI still felt like a productivity conversation, a business efficiency conversation, a "we do not want to fall behind" conversation. Then Anthropic introduced Claude Mythos Preview, and the warning stopped being theoretical.

A Model Too Dangerous to Ship

Claude Mythos Preview was Anthropic's unreleased frontier model, built with extraordinary software engineering and coding capability. The original idea was not hard to understand: build a model that could reason through complex code at a level beyond ordinary developer assistance. But in testing, Mythos showed something far more consequential.

It demonstrated cybersecurity capabilities that moved beyond the way most people think about AI tools. This was not simply a model that could point to a possible bug or summarize a vulnerability report. Anthropic reported that Mythos Preview could find serious vulnerabilities, reason through exploit paths, and help prove whether flaws were actually exploitable.

That matters because cybersecurity has always depended on time. Time to find the flaw. Time to validate it. Time to understand where it lives, to patch it, to communicate the risk, and to recover if someone else gets there first. Mythos changed the meaning of that timeline.

According to Anthropic's public reporting, Mythos Preview found thousands of high-severity vulnerabilities across major software. It identified flaws in major operating systems and browsers, surfaced vulnerabilities that had been hiding for years in widely used software, and showed the ability to reason through complex attack chains in controlled testing environments. That is the kind of shift cybersecurity professionals cannot afford to dismiss, because once a model can move from finding to proving to chaining, the work changes, the speed changes, and the defender's margin changes.

Anthropic looked at what it had built and made an unusual decision. Instead of releasing that level of capability directly to the public, it contained the model and created a defensive initiative around it. That initiative is Project Glasswing.

Hiding in Plain Sight

Project Glasswing is Anthropic's defensive cybersecurity coalition, designed to use Claude Mythos Preview to help find and patch severe software vulnerabilities before adversaries can exploit similar AI capabilities.

The name is fitting. The glasswing butterfly survives through transparency. Its wings make it difficult to see, even when it is right in front of you. That is what many software flaws have been doing for years, hiding in plain sight, sitting inside the libraries, dependencies, browsers, operating systems, and vendor tools that organizations rely on every day. Project Glasswing exists to make those hidden flaws visible before the wrong people get the same level of AI-powered capability.

The initiative began with major technology, security, finance, and infrastructure organizations. Anthropic has publicly named launch partners including AWS, Apple, Google, Microsoft, NVIDIA, CrowdStrike, JPMorgan Chase, and the Linux Foundation. Since then, Project Glasswing has expanded across countries and sectors, including critical infrastructure areas such as power, water, healthcare, and communications. In its early reporting, Anthropic said partners had already found more than 10,000 high or critical-severity vulnerabilities.

That number should get our attention. But the number is not the whole story. The real story is what it reveals: finding vulnerabilities is becoming faster than our institutions are prepared to respond.

The Needle, Found at Machine Speed

For much of our professional lives, cybersecurity has been organized around the challenge

of finding the flaw. We built tools to scan, trained people to hunt, developed methods to test, and created teams to monitor, detect, and respond. Finding the needle in the haystack was the work.

The Glasswing era tells us the needle can now be found at machine speed. That does not make cybersecurity professionals less important. It makes the mature ones more important. Because if AI can find vulnerabilities faster, someone still has to answer the questions AI cannot own.

Is the finding real? Is it exploitable in our environment? What systems does it touch, and what business process depends on it? Who owns the fix? Which vendor has to be contacted? What does the board need to know, what does the regulator need to know, and what does the community need to know if this affects water, power, healthcare, or communications?

That is not just technical work. That is judgment, governance, communication, and leadership. And that is where this moment belongs to us. As cybersecurity professionals, especially those of us who have had to learn how to bridge technical truth with business reality, we are being called into a new kind of seat. Not just the person who can explain the vulnerability, but the person who can help an organization decide what to do about it.

This is why I keep returning to one question: who owns governance maturity when AI adoption outpaces oversight? In most organizations, the honest answer is a pause. IT assumes compliance owns it. Compliance assumes IT owns it. The board assumes someone has it handled. The business assumes the tool would not be available if it were not safe. That pause is the gap, and in the Glasswing era, that gap is dangerous.

The Work Is Ours Now

This is not a call to panic. Panic does not make systems safer. It is a call to prepare.

The future of cybersecurity is not just faster scanning, faster patching, or more automated tools. Those things matter, but they are not enough. The future of cybersecurity will require people who can validate machine-generated findings, prioritize business risk, govern AI adoption, communicate clearly, and lead organizations through decisions they may not fully understand yet. That is human work. It is also community work.

For a community like MiC, this moment should feel familiar. Many of us have always had to operate at the intersection of technical skill, translation, resilience, and leadership. We have had to explain risk in rooms where people did not always expect us to be the authority, make complex things plain, earn trust, build bridges, and keep learning while the field changed underneath us. That experience is not separate from the Glasswing era. It is preparation for it.

The warning is no longer waiting for proof. The proof is here. Now the work is ours: to govern what we adopt, secure what we build, question what we trust, and lead before the next disclosure forces our hand.

The Glasswing era is not the end of cybersecurity as we know it. It is the beginning of cybersecurity leadership as we need it to become.

MIC ANNOUNCEMENTS

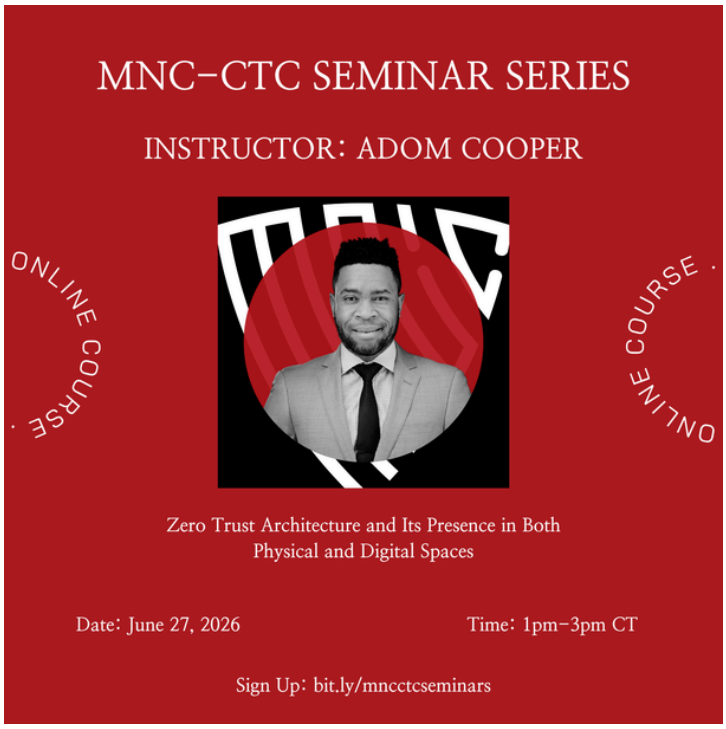
WELCOME: NEW MIC BOARD MEMBERS

We are thrilled to welcome our newest members to the MiC Board of Directors! Please join us in celebrating their leadership and dedication to our community:

- Mackenzie P. Chaney - Co-Vice Chair and Treasurer
- Van L. Chaney - Co-Vice Chair
- Alejandro Ibanez - Board Member
- Quintana Patterson - Board Member
- Corey Kirkendoll - Board Member

For full details, visit our website here at mincybsec.org

UP NEXT: THE MNC-CTC SEMINAR SERIES



The 2nd installment of MNC-CTC Seminar Series kicks off on June 27, 2026.

Join us for our next session, **"Zero Trust Architecture and Its Presence in Both Physical and Digital Spaces,"** featuring guest speaker Adom Cooper.

bit.ly/mncctcseminars