SEPTEMBER 2025

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

The theme for this quarter's newsletter is unity in action. In many contexts, unity seems to be in short supply. Many societies are struggling to find any unity across political, regional, cultural, or international divides, including in efforts to combat malicious cyber activity. Discord is the order of the day, and malicious actors are quite content to profit from the current state of affairs.

Why is achieving unity so hard? One problem is that we often conflate unity with uniformity. While related words in English, they represent different concepts. Uniformity implies that beliefs, appearances, and approaches are the same across a group, whatever that group is made up of. Unity means working together toward a common end. While I may want uniformity in my group martial arts demonstrations, it doesn't work well in an association of rival cybersecurity companies – and, I would argue, it's not even desirable. Unity, though, that's more achievable. And it produces results.

Another problem is that we forget the "in action" part of the phrase. It's not unity for the sake of being unified, or even unity of beliefs or perspectives. CTA's unity occurs as part of actions: protecting end users, disrupting malicious actors, and raising the level of cybersecurity across the digital ecosystem. CTA's unity emerges through the actions of our members, whether that action is sharing of threat intelligence in various modes, from automated data to finished reports to conversations. It emerges through combined support to international efforts, such as the Cyber Defense Assistance Collaborative, which provides defensive cybersecurity assistance to Ukraine or through the sponsorship of conferences on the art and science of threat intelligence sharing that draw researchers from all over the world.

These examples highlight a strange fact: CTA's unity in action relies on differences in our members. While this idea may seem like a contradiction, in fact it is CTA's core strength. The variance in member business models, national headquarters, customer bases, and technologies creates CTA's value for its members. Without these differences, unity in action would have limited value. By harnessing the differences, the concept of unity in action becomes a force multiplier.

Unity in action does not rely on uniformity or total consensus. As you read this newsletter, you'll see plenty of differences. Instead, unity in action is an emergent property of an organization like CTA, if it's built correctly. As always, thank you to those companies who are on this journey with us. For those of you whose organizations haven't joined CTA yet, there's still plenty of room. Come join us and experience the power of unity in action first hand. We may not always agree on everything, but we will be unified in our actions.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>17 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	50%
IP ADDRESS	16%
DOMAIN NAME	3%
URL	5%
NETWORK TRAFFIC	15%
FILE PROPERTIES	6%
HOST	5%

TOTAL EARLY SHARES

3-5
PER WEEK

1,300+

Unity in *Action*

PROTECTING THOSE WHO SERVE: THE CRITICAL CYBERSECURITY CRISIS FACING AMERICA'S NGOS

NGO-ISAC
BETTER TOGETHER

Every day, nonprofits provide essential services—educating our children, treating the sick, and strengthening our communities. Unlike large corporations, these mission-driven organizations lack the resources to defend against sophisticated cyber threats or make security investments against profit margins.

The NGO Information Sharing and Analysis Center (ISAC) exists to change this. We unite 400 NGO members and 50 vendor partners to boost cybersecurity maturity through intelligence sharing, best practices, and education. Our community spans major organizations with dedicated security staff to small nonprofits with bare-bones IT resources—united only by our nonprofit status and commitment to help each other.

Our collaborative approach works. Members and vendors share through weekly briefings and online forums. Even competing vendors generously contribute time and resources to help our community. We are able to coordinate responses across our sector. The best example is the work we did with Microsoft against Russian APT Star Blizzard's attacks on NGOs.

However, recent months have brought unprecedented challenges. Beyond traditional cyber threats, many NGOs now face government-led campaigns targeting their staff and mission. This has led to:

- Complete organizational shutdowns
- Building seizures
- Massive staff reductions (one member dropped from 1,200 to 200 employees)
- Haphazard contract cancellations and restorations that make planning impossible

These attacks include defunding counterterrorism detention facilities, nutrition programs for starving children (while still funding food that now rots unused), and organizations protecting critical civic infrastructure. Such cuts defy logic and endanger American interests. It also weakens this sector's cybersecurity, as organizations focus resources on survival. And since we live in an interconnected world, these reductions make everyone's cybersecurity weaker.

The sector needs immediate and ongoing help. We urgently need to protect organizations that cannot protect themselves.

Join us. Visit NGOISAC.org and use our Join form to become a member or partner. Help us defend the organizations that defend our communities.

BY IAN GOTTESMAN
CEO
NGO-ISAC

UNITY IN ACTION: DEFENSE BENEFITTING EVERYONE

Scitum | TELMEX está contigo

In the world of cybersecurity, we are all here to make the world a better place. Our work reduces the risks of cybercrime so people can live normally and happily. No one can do this alone. In this field, no individual or organization is self-sufficient. Attackers keep searching for blind spots across cybersecurity tools and sectors, and the only way we all improve is by helping one another.

When someone shares a blog post or lessons from an incident, the tactics, techniques, and procedures they share become a light that helps others detect and stop similar attacks. However, not every insight belongs in a public post. Oversharing can tip off an attacker or expose details that put other organizations at risk. That is where the Cyber Threat Alliance comes in, because some of the most valuable intelligence emerges in the heat of incident response. The CTA provides a trusted space where sensitive details can be shared securely, with confidence that the person on the other side is a highly skilled, deeply committed peer, not a criminal. You can never fully guarantee this when publishing openly.

These bonds of cooperation are not built overnight. Trust must be built before the crisis. You show up, you contribute, you listen, and you earn the confidence of others. If people do not trust you, they will not share the insights that could help you prevent an attack. When we share threat intelligence from Latin America, we help global partners prepare for attacks they might not have seen yet. In return, they share what we would not otherwise notice, which makes us better at defending the organizations we serve.

This is what unity in action looks like. It benefits everyone. It is powered by trust and by a shared purpose that is larger than any one company. We defend people we may never meet. We turn lessons learned the hard way into protection for others. Step by step, together, we move closer to a safer world.

BY IMELDA FLORES
HEAD OF SCILABS
SCITUM

UNITY IN ACTION: TURNING PROBLEMS INTO PROGRESS

In today's turbulent cyberspace, unity is no longer a lofty ideal—it is a strategic necessity. As the digital landscape grows more volatile, the only way to build resilience is through collaborative action, shared responsibility, and proactive engagement across individuals, organizations, and nations.

Organizations like the CTA and ISACs exemplify this principle. Competitors in the cybersecurity space are setting aside rivalry to share threat intelligence—preventing widespread damage and strengthening the collective security posture of our digital ecosystem.

At the Cyber Future Foundation (CFF), we've long embraced this ethos. From the early days of the Afghan crisis to the ongoing cybersecurity challenges faced by humanitarian organizations, our members have consistently answered the call. Quietly, effectively, and without hesitation.

But the stakes are rising. The convergence of geopolitical shifts, domestic transformations, and emerging technologies demands a new level of unity—one that transcends election cycles and short-term gains. Resilience now depends on investments in infrastructure, education, and digital sovereignty that can withstand global shocks.

This is not just a call to governments or tech giants. It's a call to all of us—to build consensus across sectors and borders, to ensure diverse voices are heard in shaping the future of cyberspace, and to move from admiring problems to solving them.

The partnership between CFF and CTA is a model of what's possible when commitment, consensus, and conscience align. Together, we can shift the narrative from fragmentation to fortification.

We're ready. Are you?

BY KATHERINE THOMPSON
CHIEF OPERATING OFFICER
CYBER FUTURE FOUNDATION

OCTOBER 8, 2025

CyberNext★DC

Cybersecurity Coalition

CYBER THREAT ALLIANCE

UNITY IN ACTION: STRENGTHENING CUSTOMER SECURITY THROUGH COLLABORATION

At the CTA, we empower our members by facilitating the exchange of timely, relevant, and actionable threat intelligence. Through our trusted sharing platform, members gain access to enriched data sets, early insights into emerging threats, and exclusive research on malicious activity. This collaborative approach enables organizations to validate and enhance their existing intelligence, improving their ability to detect and prevent threats and ultimately, better protect their customers.

CTA members are recognized leaders in cybersecurity, united by a shared commitment to securing the global digital ecosystem. By contributing contextualized intelligence, members gain a more comprehensive view of the threat landscape, one that spans industries and geography.

Elevate Your Brand Among Cybersecurity Leaders

Joining CTA signals to stakeholders that your organization values collaboration, transparency, and the power of shared intelligence. It demonstrates confidence in the quality of your threat data and the expertise of your research teams.

Our members believe that cybersecurity should compete on their technology innovation and impact, not on hoarding threat indicators. By sharing IOCs and technical context, we raise the bar for the entire industry and drive stronger, more resilient defenses.

Gain Context-Rich Insights Into Cyber Threats

Each week, CTA processes millions of observables, each accompanied by essential contextual metadata. Members can also contribute additional insights to enrich the collective understanding of malicious activity.

This depth of context helps answer critical questions: What are the tactics used? Who is behind the attack? What are they targeting? Where and when is it happening? Why is it significant? All this enables members to prioritize defenses and respond with precision.

Leverage Global Perspectives to Strengthen Defenses

CTA's diverse membership, which includes cybersecurity vendors, MSSPs, ISPs, telcos, and platforms, brings a wide range of visibility and expertise. With coverage across regions and industries, our members contribute unique insights into threats affecting different parts of the world.

By pooling this intelligence, members expand their situational awareness and increase the cost of operations for adversaries, making it harder for them to succeed.

Join CTA – Working Together for the Greater Good

CTA members are shaping a safer digital future by sharing intelligence that benefits everyone. For organizations that produce and consume threat intelligence, this collaboration is not just valuable, it is essential.

CYBER THREAT ALLIANCE

BY JEANNETTE JARVIS
CHIEF BUSINESS OFFICER
CYBER THREAT ALLIANCE

MEMBER SPOTLIGHT: SONICWALL®

WHY DID SONICWALL JOIN CTA?

SonicWall joined CTA in order to be a part of a broader cybersecurity community and gain additional perspective of threat landscape as visible by other members. Also, SonicWall wanted to make its own contribution to the community by sharing its own threat intelligence with others.

HOW DOES MEMBERSHIP IN CTA HELP SONICWALLPROVIDE GREATER SECURITY FOR CUSTOMERS?

By being a member of CTA, SonicWall gains access to an additional set of high-quality threat data. Then by integrating CTA intelligence into its products, SonicWall can detect and block threats more quickly. Having visibility into shared threat intelligence provided by other CTA members enables SonicWall to correlate data across multiple data sources thus improving accuracy of its own threat detection.

HOW DO YOU SEE CTA FITTING INTO THE BROADER CYBERSECURITY LANDSCAPE?

CTA works with government agencies hence enhancing national and global cyber defense. CTA supports multi-vendor and public-private collaboration models where the end goal is to provide access to cybersecurity information through shared knowledge.

WHAT VALUE DO YOU GET FROM CTA?

Mainly information sharing and being able to quickly gain access to "in-the-know" 3rd party perspective quickly on the hottest issues (high visibility/impact vulnerabilities, etc.) that come up in the daily cybersecurity workflows.

WHY IS INFORMATION SHARING IMPORTANT IN TODAY'S CYBERSECURITY ENVIRONMENT?

One vendor does not have the presence and access to every data point or an insight on the latest incident of interest. Only through community sharing can all vendors have access to necessary information to provide the best protection to its customers.

WHAT ARE YOU MOST EXCITED ABOUT IN TERMS OF THE WORK YOU HAVE BEEN ABLE TO DO THROUGH CTA?

The most exciting part is being able to collaborate with the best-of-the-best cybersecurity vendors and to offer and contribute our own data to the entire CTA membership base.

WHAT DO YOU SEE AS THE MOST SIGNIFICANT EMERGING CYBERSECURITY CHALLENGES AND HOW CAN CTA HELP TO MITIGATE THESE CONCERNS?

The biggest emerging cybersecurity challenges would be the speed of threat evolution (especially with threat actors utilizing more powerful AI-based systems), increase in sophistication of cyber threats especially with extra sponsorship from nation-states actors, lack of qualified resources to deal with such threats, fragmented threat intelligence. CTA's best tool to attempt to mitigate these concerns is to bring the best cybersecurity minds/ vendors together and address those challenges through collaboration and sharing of the best tools/techniques and the most recent/accurate data.

WHERE DO YOU SEE CTA IN 5 YEARS?

We see CTA growing and gaining more members across additional industry sectors and geographical regions.

ANYTHING ELSE YOU WOULD LIKE TO ADD?

Given its reputation and trust of CTA in the industry and threat research community, being accepted as a member strengthens SonicWall position as a trusted cybersecurity vendor in the industry.

CTA HOSTED WEBINARS

Water, water everywhere, nor any drop to drink.

That quote from Coleridge's "The Rime of the Ancient Mariner" aptly describes the situation with cyber metrics: we are awash in data yet have trouble measuring cybersecurity, particularly at the national level.

Join us on September 10th for a webinar on cyber metrics — **What Gets Measured, Gets Done: A National Dashboard for Cybersecurity.**

In this webinar, Michael Daniel (CTA), Jason Healey (Columbia University), Wade Baker (Cyentia), Chris Wysopal (Veracode), and Alex Pinto (Verizon) will discuss this long-standing problem and what we can do about it. The panel will examine what makes for good ecosystem metrics, which ones would be both informative and practical for a whole country, and how we could use them to inform decisions at the national level.

We'll also talk about what might be some good news for cyber defenders when you start looking at some the proposed metrics. While we may never be able to measure cybersecurity with precision, metrics can make our decision-making processes better.

Can't make it? Catch this webinar — and all CTA-hosted webinars — on demand on our YouTube channel.