DECEMBER 2025

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

Collective Strength, Collective Impact. As a theme for a cybersecurity newsletter, it does not seem all that radical. The cybersecurity industry talks about sharing and collaboration all the time. Yet, when you think about it, the statement is actually highly unusual. For industries as fiercely competitive as cybersecurity, collaboration is usually an anathema. The cybersecurity industry stands out for having collaborative activities occur in the same space as fierce competition.

Why does the industry operate in this manner? A combination of factors drives the industry's dual nature, including its roots in government, an intelligent adversary, and the network effects of information technology. Taken together, they create a powerful incentive for collaboration.

The cybersecurity industry partially grew out of the national security and law enforcement areas within governments. These areas are highly mission driven and that culture carries over into private sector cybersecurity companies when they are formed. Further, many of the people who work in the industry have spent time in government service. This strong service and mission ethos helps create a willingness to work together. The other source for the cybersecurity industry is the IT sector, which has cultural elements that lean towards a mission focus and a desire to make society better. These twin cultural foundations encourage companies to take a collaborative approach to their work.

Combating intelligent adversaries forms the second unusual feature of the cybersecurity industry. For most organizations, they are not fighting "malicious actors" as part of their business model. In fact, governments are the only ones combatting adversaries in most societies. Yet, for the cybersecurity industry, the fight is integral to what they do. In turn, this focus on adversaries means "competitors" are also allies against a common threat – a powerful incentive for collective action.

Finally, the very nature of networked information technology encourages collaboration. The benefits of connectivity and collaboration grow rapidly as the network size increases. This effect carries over into the cybersecurity space, meaning that collaboration provides direct benefits to the participants as well as the network as a whole. These network effects help maintain a positive feedback loop for collective action.

Despite the power of these factors, we should not assume that the industry has to maintain this culture of "collective strength." These elements could be eroded or ignored. That's why we want to highlight this aspect of the industry and the benefits it provides. As we head towards the end of the year, we all need a reminder of the benefits that derive from having a collaboratively competitive (or a competitively collaborative) industry structure. We should not take this structure for granted and instead do everything we can to reinforce it.

The articles in this newsletter showcase the different ways our members exhibit "Collective Strength, Collective Impact." They highlight the diverse ways that companies and individuals implement this concept. And I hope they inspire you to continue the hard work of cybersecurity.

J. Michael Daniel

President & CEO, Cyber Threat Alliance

CONGRATULATIONS, MICHAEL!

We are pleased to share that **Michael Daniel, CTA President and CEO**, was awarded the **Cyber Future Foundation Cyber Futurist Award!**

The Cyber Future Foundation advances global cybersecurity through innovative programs, thought leadership, and collaborative initiatives that protect humanitarian missions, govern AI responsibly, and build cyber resilience worldwide.

We are honored to celebrate Michael and his recognition at CTA!

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>16 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

1,350+

K7 COMPUTING

CTA Member Feature

NO MAN'S LAND: BRIDGING THE DIVIDE IN CYBERDEFENSE

Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.

— Sun Tzu

In today's digital battlefield, governments and corporations have a certain mutual trust deficit despite facing a common cyber adversary.

Governments seek visibility and control. They advocate and legislate regulatory frameworks, demand lawful access mechanisms (often criticized as covert surveillance), and conduct offensive cyber operations against hostile states and criminal networks while fortifying the country's cyberdefense. Corporations, on the other hand, design and maintain digital infrastructure, steward vast reservoirs of user data, and frequently resist government intrusion citing, for example, innovation, privacy rights, and global competitiveness. The result is a fragmented defense ecosystem with blurred accountability.

The stakes are monumental: safeguarding national security, strengthening the economy, preserving consumer privacy, protecting intellectual property, and defending critical infrastructure against increasingly sophisticated adversaries. But, who secures the cloud servers storing citizen data? Who responds when ransomware cripples healthcare systems? Who bears responsibility when state-sponsored actors breach private enterprises? Who will deal with the dearth of skilled cybersecurity personnel?

Some notable incidents have underscored the interdependence of governments and enterprise. What might begin as a corporate cybersecurity crisis could rapidly escalate into a national cybersecurity meltdown. In these instances, the response can be slow, coordination fragmented, and accountability diffuse — a case study in the dangers of operating without a coherent, cooperative cybersecurity framework between government and enterprise given that neither entity, alone, can close the loop between protection, remediation, regulatory compliance and legal action.

Effective partnerships between government and industry would convert combined intelligence, authority and action into a sustainable and hard-hitting defense.

The CTA is a multi-stakeholder cybersecurity alliance that helps bring together governments, public agencies (including LEAs), private sector operators, and independent cybersecurity organizations against a common adversary.

Until governments, corporations and law enforcement agencies establish shared frameworks, align incentives, and bridge the talent gap, the digital frontier will remain dangerously exposed — a no-man's land with ill-defined boundaries and grey rules. Such partnerships ensure that one does not have to choose between security and authority.

Scaling and standardizing alliances such as the CTA, along with active Government participation, would materially reduce response times, provide the necessary clarity on accountability, and raise baseline resilience across critical sectors.

BY RATHNA KALIDAS
SENIOR PRODUCT MANAGER
K7 COMPUTING

IT ISAC
CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

CTA Partner Feature

THE POWER OF SHARING: HOW ISACS STRENGTHEN COLLECTIVE SECURITY

The increasingly interconnected fabric of our technology ecosystem brings with it a growing set of cyber and physical risks. Adversaries are not only collaborating more effectively than ever, they are leveraging AI to accelerate the development and deployment of new attack techniques.

At the same time, corporate security budgets are being squeezed. Regulatory demands continue to shift resources from security toward compliance, even as organizations face broader cost-containment pressures. Compounding this challenge, federal support for several cornerstone cybersecurity programs have weakened. In today's evolving threat and business environments, collaboration is not just beneficial—it is essential.

Twenty years ago, many organizations handled threats in isolation, tackling problems with limited visibility into what their peers or other organizations were facing. This defense-in-isolation model is no longer a viable option. Companies that are not collaborating with their peers are putting themselves at unnecessary risk. Thanks to the development of a vast network of Information Sharing and Analysis Centers (ISACs) within critical infrastructure sectors, this collective approach to defense makes prevention easier, detection faster, and recovery more manageable.

This unified defense model spans the entire critical infrastructure landscape. The National Council of ISACs (NCI) facilitates analysis and joint responses across ISACs. By connecting these communities, individual insights become shared intelligence, allowing sectors to strengthen one another's defenses. The power of this network is exemplified in the jointly authored reports or alerts, such as the recent Scattered Spider Guidance Report, in which multiple ISACs combined research, analysis, and expertise to develop clear actionable recommendations.

But collective strength is not limited to collaboration among ISACs. It also grows through strong partnerships with government agencies and industry trade associations. Public-private partnerships accelerate the flow of information, helping all parties spot trends earlier and with greater precision. Industry associations provide unique insights, connecting ISACs to a broader network of organizations for resource exchange and faster information dissemination.

A shared-security approach recognizes a simple truth: no organization can defend itself effectively on its own. In a time of constrained budgets, sophisticated threats, and reduced federal government engagement, threat intelligence sharing networks serve as a force multiplier, enhancing security and resilience. Threat actors are actively working together to attack. Network defenders must join forces to protect.

BY SCOTT ALGEIER
EXECUTIVE DIRECTOR
IT-ISAC

SOPHOS
DEFEAT CYBERATTACKS

WHEN SECURITY TOOLS BECOME TARGETS

The cybersecurity industry continues to grapple with deep product security challenges, as recent incidents involving F5 and SonicWall have highlighted. While much of the industry's focus has traditionally been on defending organizations from external threats, it is becoming increasingly clear that the tools we rely on are themselves being targeted by sophisticated adversaries.

These are not opportunistic attacks. They are part of a long-term, deliberate strategy that can involve years of research to deeply understand product architectures and exploit them. In some cases, attackers appear to have gained access to internal documentation or even source code through direct breaches of vendor engineering environments.

Sophos has first-hand experience with this challenge. As detailed in our Pacific Rim research last year, following our acquisition of Cyberoam, we encountered evidence of a targeted campaign that exploited vulnerabilities with a detailed understanding of our product design. Other vendors have reported similar experiences, suggesting this may represent a wider and underappreciated issue across the industry.

As Ollie Whitehouse, Chief Technology Officer of the UK's National Cyber Security Centre (NCSC), has observed, this problem is not only technical—it is also one of market incentives. Buyers have a crucial role to play in driving change. Rather than punishing vendors who are transparent about breaches, we should encourage and reward those who demonstrate a genuine commitment to secure-by-design principles and openness about their internal security practices.

Practical steps buyers can take include:

- **Ask** vendors to share their internal security roadmap and look beyond surface-level assurances
- **Review** organizational charts to confirm a well-resourced internal security function led by a CISO or equivalent who has a meaningful voice in decision-making
- **Look** for a clear Vulnerability Disclosure Policy supported by an active bug bounty program

Ultimately, the industry must evolve to value security within its products as highly as it values security products themselves. Only by aligning incentives, fostering transparency, and supporting those who invest in product resilience can we collectively strengthen the foundations of our digital defenses.

BY ROSS MCKERCHAR
CISO AND VICE PRESIDENT
SOPHOS X-OPS

COLLECTIVE STRENGTH, COLLECTIVE IMPACT

By Vincent Weafer, CTA Champion and Engineering and Technology Executive

In my 25+ years of experience in the cybersecurity and now cyber insurance industry, I've come to realize that while individual resilience matters,- the collective resilience of the community or extended supply chain is what is truly important. The pace and scale of today's attacks make it clear that no single organization, the enterprise, cybersecurity vendor or insurer can see the full picture alone. Our true advantage comes from **how effectively we share what we know** – converting isolated incidents into systemwide defense improvements.

Over the past few years, we've seen encouraging progress toward that goal. The Cyber Threat Alliance (CTA) and Financial Services- Information Sharing and Analysis Center (FS ISAC) are both mature organizations and exemplify real-time, structured intelligence-sharing across cybersecurity industries. The insurance industry is also moving beyond standalone reports toward genuine data-driven collaboration. Insurers, risk managers and cybersecurity teams are increasingly engaging in **anonymized telemetry sharing**, root-cause pattern analysis and aggregated loss-trend modeling to help anticipate systemic threats. These aren't just after-action reflections – they are mechanisms for prevention, early detection and prioritized mitigation.

For example, CyberAcuView was established by leading cyber insurers to create aggregated and anonymized industry-data products. Similarly, NetDiligence publishes its annual Cyber Claims Study, which aggregates more than 10,000 cyber insurance claims drawn from multiple insurers and brokers. We know from our own data at Travelers that organizations that meaningfully engage with risk advisory services informed by such data insights are less likely to experience a cyber breach.

Three major benefits of this collaboration stand out:

1. **Sharper insight into risk vectors** – When claims data, exposed vulnerabilities and attack playbooks are shared, smaller companies gain access to the kind of visibility previously reserved for large corporations. Instead of guessing which control matters most, they learn from thousands of peer incidents.
2. **Prioritized, evidence-based controls** – By distilling the aggregated root-causes of past losses, insurers and security teams can recommend a short list of high-impact controls (for example, MFA implementation and patch management for known exploitable vulnerabilities) that can yield outsized benefit for organizations that may lack advanced security teams.
3. **Democratized resilience** – Smaller organizations often lack in-house cyber threat intelligence or data science resources. By participating in or benefiting from industry-wide datasets, they effectively "stand on the shoulders" of many others. Their individual resilience is amplified by the collective.

Standardizing how the cybersecurity industry anonymizes, normalizes and shares data remains a work in progress and isn't without its challenges. Trust frameworks must be put in place to govern data anonymization. The data-taxonomy needs to be standardized to enable consistent and scalable operations and legal/competitive considerations must be managed throughout the process. But the alternative is fragmented defense – and in the face of the threat landscape that businesses face today, that's not viable.

The final piece of the puzzle is how we get that collective intelligence out to our customers via our products, solutions and services. At Travelers, we believe that cyber insurance goes beyond coverage. We actively communicate with policyholders and brokers, sharing timely recommendations and guidance to help strengthen their cyber resilience before, during and after an incident. This collaborative approach builds collective resilience, helping organizations anticipate, withstand and recover from evolving cyber threats.

The threat landscape and attacker ecosystem are constantly evolving and so must our defense. Through transparent data exchange, joint learning and prioritized remediation, we convert many separate failures into one stronger ecosystem. That is the essence of **Collective Strength – Collective Impact:** turning shared insight into shared protection and transforming an industry's knowledge into resilience for all.

BY VINCENT WEAFER
CTO
CORVUS INSURANCE

MEMBER SPOTLIGHT:

Penta SECURITY

WHY DID PENTA SECURITY JOIN CTA?

CTA is an alliance where members share vast amounts of cybersecurity information. As the market leader in South Korea, Penta Security (Cloudbric) was attracted to the opportunity to contribute Asian cybersecurity intelligence while gaining access to the latest insights from the European, North American, and Middle Eastern markets where we are expanding. Furthermore, we joined CTA in 2022 because the shared data and latest cybersecurity intelligence enable us to build a stronger security environment, and we continue to actively share information to this day.

HOW DOES MEMBERSHIP IN CTA HELP PENTA SECURITY PROVIDE GREATER SECURITY FOR CUSTOMERS?

Through CTA membership, we've gained insights from global cybersecurity industry experts. This enables us to identify new attack patterns and zero-day vulnerability information early and incorporate them into our products and services. Particularly for globally spreading threats, we can share experiences and response strategies with other members to proactively protect our customers. As a result, we have not only enhanced customer trust but also contributed to strengthening the entire global cybersecurity ecosystem.

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

The first is AI security. As AI technology advances rapidly, attackers are also exploiting AI to create more sophisticated phishing emails and conduct automated attacks. Simultaneously, as many companies adopt AI systems, they are exposed to new threats. We also recognize these AI security threats and are actively preparing countermeasures.

The second is cloud security. With global business expansion, many companies are transitioning from on-premises to cloud environments. Consequently, attacks exploiting cloud vulnerabilities are surging. CTA members experience these emerging threats in real-time across their respective markets and customer environments. By sharing the latest attack examples and effective response strategies through the CTA platform, we can build proactive defense systems before attackers make their moves.

WHAT DOES PENTA SECURITY CONSIDER MOST IMPORTANT IN THE CYBERSECURITY LANDSCAPE?

We consider data encryption as the last line of defense and the most critical element of security. No matter how sophisticated defense solutions are deployed, situations can arise where attackers eventually breach defenses and steal data. However, if critical data is strongly encrypted and encryption keys are securely managed, even if data is leaked, attackers cannot practically utilize it. Considering the enormous costs of lost customer trust, legal liabilities, and corporate reputation recovery after a data breach, investing in encryption technology upfront is a far more effective and economical choice.

At Penta Security we are looking forward to driving significant value through our continued strategic collaboration with CTA.

paloalto® NETWORKS

COLLECTIVE STRENGTH, COLLECTIVE IMPACT

Cybersecurity is a team sport. As threats grow more sophisticated and move globally, collaboration isn't optional—it's essential. That's why Palo Alto Networks, and Unit 42, are proud to be founding members of the CTA, an organization built on one powerful idea: we're stronger together.

Through the CTA, cybersecurity industry leaders share threat intelligence in near real time — enabling faster detection, deeper analysis, and coordinated action across member organizations. Unit 42 plays a leading role in this collaboration, contributing timely, high-confidence threat intelligence and helping to shape standards for responsible sharing and joint response. Our collaboration doesn't stop at data. Unit 42 experts actively participate in CTA committees, working together to shape standards for intelligence sharing, attribution, and coordinated responses.

The impact of this collective strength is tangible. Coordinated actions demonstrate what's possible when competitive boundaries give way to a shared sense of purpose. It's not just about sharing data—it's about sharing trust, expertise, and responsibility for protecting the digital world.

Beyond intelligence sharing, member organizations actively support CTA initiatives that advance education, outreach, and cross-industry trust. Whether through conference panels, workshops, or day-to-day collaboration, we're committed to amplifying the voice of the defender community.

One of our researchers recently uncovered telemetry pointing to possible compromise and malicious activity involving another CTA member's product. Thanks to the trusted relationships fostered through the alliance, we connected with the right people immediately, shared what we'd found, and helped them act quickly. This shows how collaboration — even among competitors — has a real, positive impact on securing the digital ecosystem.

At Palo Alto Networks, we believe that collective strength drives collective impact. When we share intelligence, expertise, and purpose, we do more than stay ahead of threats—we move the entire cybersecurity ecosystem forward. Every new intelligence contribution, every CTA collaboration, every shared success story reinforces a simple truth—when we unite as a community, we don't just respond to threats; we redefine what it means to be secure.

BY KATHI WHITBEY
LEAD PRINCIPAL PM,
PALO ALTO NETWORKS, UNIT 42