MARCH 2021

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

Friends of CTA,

In this newsletter, we are honoring International Women's Day. We have interviewed six women associated with the Cyber Threat Alliance, profiling their professional achievements. I am always interested in the journeys people have taken to arrive at a career in cybersecurity, because the paths are so varied. There's no standard way into this business. You will see that variation in play in the stories on the last few pages of this newsletter.

I am very proud that CTA could profile these six women leaders. Their successes speak to the value of diversity, equity, and inclusiveness (DEI) in the cybersecurity workforce. Unfortunately, though, we have a lot more work to do as an industry. The cybersecurity industry, and technology more broadly, remains too homogenous – if we are going to outwit, outmaneuver, and outflank the criminals and other malicious actors, we need diversity of thought, geography, culture, and viewpoint. While DEI promotes social justice, it is also smart business and good for the digital ecosystem.

For all these reasons, CTA is committed to expanding DEI in cybersecurity. We are participating in the Aspen Institute's DEI initiative. We are supporting efforts to change terminology that reflects a less inclusive past (e.g., substituting "blocklist" for "blacklist"). We have created special recruitment efforts to connect with potential member companies across multiple regions. For CTA-sponsored conference tracks, we keep DEI front-of-mind as we assemble speakers and panels for two reasons. First, more diverse panels are simply better panels, generating more informative and creative discussions. Second, we want to showcase industry leaders whose backgrounds and experiences allow them to serve effectively as role models for creating an even more diverse next generation of cybersecurity talent. I know that we can do more, though, and we will continue to search for those opportunities.

Like information sharing, talking about DEI in the abstract is easy. Taking concrete actions that improve DEI is hard, requiring self-awareness, reflection, and commitment. CTA is built to take on the hard problem of information sharing; in the long run, if we want to achieve our goal of raising the level of cybersecurity across the digital ecosystem, we must take on this hard problem too.

Finally, in line with efforts to increase geographic diversity, I am pleased to welcome Avast, Morphisec, SecurityScorecard, and TEHTRIS to CTA. Please see the new member feature below for more details.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

FOUR NEW CTA MEMBERS + 25% GROWTH Y.O.Y.

From December 2020 through February 2021, the CTA team was delighted to be able to welcome four new members into the Alliance: **Avast**, **Morphisec**, **SecurityScorecard**, and **TEHTRIS**. This surge in membership growth takes CTA to a total of 32 member companies, a roughly 25% increase since the start 2020 and 40% increase since the beginning of 2019.

With each of these new members being headquartered in a different country — Czechia, Israel, the U.S., and France, respectively — it's clear that confidence in CTA's mission is growing and is spreading globally. Just as importantly, the industry is waking up to the fact that the value of threat intelligence sharing is enhanced by a greater level of diversity among sharing contributors, including through wider coverage across geography and industry verticals. For more details about membership, **contact us** today.

avast   MORPHISEC Moving Target Defense   SecurityScorecard   TEHTRIS FACE THE UNPREDICTABLE

YEAR-END SHARING SNAPSHOT

TOTAL OBSERVABLES SUBMITTED

>150 MILLION

SINCE FEBRUARY 2017

KILL CHAIN DIVERSITY

(2020 AVERAGE)

RECONAISSANCE	1%
WEAPONIZATION	>0%
DELIVERY	15%
EXPLOITATION	5%
INSTALLATION	42%
COMMAND + CONTROL	27%
ACTIONS ON OBJECTIVES	9%

NOTE: Every IoC submitted to CTA must be accompanied by a kill chain phase.

TOTAL EARLY SHARES

3-5

PER WEEK

375+

SINCE THE START OF OUR EARLY SHARING PROGRAM IN MAY 2018

Collaborative work with CTA's partner organizations continues to generate impact

PARTNERSHIPS YIELD POLICY IMPACT

Throughout 2020 and into this new year, CTA staff have been working closely with various partner organizations to drive progress on a range of high-profile cybersecurity policy issues. CTA's contributions to these projects help drive recognition for the Alliance as a hub for thought leadership in the cybersecurity space, and ensure the presence of a balanced, industry-oriented voice at the discussion table.

WORLD ECONOMIC FORUM (WEF)

As a participant in both the World Economic Forum (WEF) **Partnership Against Cybercrime** and **Global Futures Council on Cybersecurity**, CTA enjoys a prominent position at the WEF that enables us to advocate for a safer, more resilient digital ecosystem. Alongside several CTA members, we are forging ahead in the implementation of the **recommendations** delivered by the WEF Partnership on Cybercrime at the end of 2020 and look forward to sharing more details about how CTA intends to support a more robust, collaborative approach to countering cybercrime with our wider community over the coming months.

ASPEN INSTITUTE

CTA contributes to both the **Aspen Cybersecurity Group** and the Institute's **Digital Diversity, Equity, and Inclusion** program. The Cybersecurity Group is made up of former government officials, academics, and industry practitioners, and seeks to deliver actionable policy recommendations for the U.S. government to improve domestic and global cybersecurity. The group has published papers on increasing the cyber workforce, improving operational collaboration, and principles for IoT device security. The Digital Diversity, Equity, and Inclusion program, meanwhile, is focused on efforts to "rebuild the digital ecosystem to be reflective of the world's diversity" through improvements to talent recruitment, hiring, retention, and promotion, as well as enhanced accountability around those issues for both private and public sectors.

NEW YORK CYBER TASK FORCE (NYCTF)

Over the past year, CTA has contributed to the efforts of the **New York Cyber Task Force** (NYCTF), based out of Columbia University's School of International and Public Affairs. Over that period, the NYCTF, which includes participants from the private sector, academia, and global civil society, has undertaken a series of workshops and scenario exercises to inform recommendations for more impactful operational collaboration at a "whole-of-nation" scale. The NYCTF concluded its work in late February.

IST RANSOMWARE TASK FORCE (RTF)

CTA was an early participant in the Ransomware Task Force (RTF) created by the Institute for Security & Technology (IST). The RTF formed in January 2021 to deliver recommendations for public and private action to tackle the growing scourge of ransomware, and it is leveraging a coalition of experts from the private sector, government, law enforcement, and global civil society to meet these goals. It expects to deliver a report in April 2021. CTA is pleased to be able to represent the interests of our members and the cybersecurity industry writ large as a part of this important initiative. To learn more and follow RTF's progress moving forward, we encourage you to visit their **website**.

Looking back on four great years

HAPPY BIRTHDAY, CTA

On January 23rd, CTA turned four years old. However, the idea of CTA goes back even further — at least to a working lunch in 2014 between Fortinet CEO, Ken Xie, and then-CEO, now Vice Chairman, of Palo Alto Networks (PAN), Mark McLaughlin. We were recently able to gather these two industry leaders, along with then McAfee CEO Chris Young (now Microsoft EVP of Business Development), for a special birthday webinar to discuss the past, present, and future of the organization that they all helped to create. You can view a recording of that webinar **here**.

> **"While I look back with pride on CTA's origins, I'm more proud that we set something up that will last."**
>
> **Chris Young**
> Fmr. CEO, McAfee

When CTA was founded, the success that we enjoy today was far from guaranteed. "CTA wanted to be global in scope, not dominated by a single country, and with a diverse membership," recalled Derek Manky, Chief of Security Insights & Global Threat Alliances at Fortinet's FortiGuard Labs in a recent **guest blog** for CTA published around the time of the organization's anniversary. Such an undertaking had to be rooted in trust, which always takes time to grow and solidify.

> **"I am yet to talk to a customer who doesn't love the idea of CTA."**
>
> **Mark McLaughlin**
> Vice Chairman, PAN

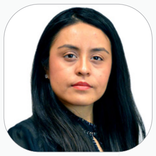
Looking back on the period around CTA's founding in another recent **guest blog**, Ryan Olson, VP Threat Intelligence at PAN's Unit 42, offered a useful reminder that "it's important not to be complacent. CTA didn't happen by accident. Industry leaders put in the time to make it work." For CTA's success to continue, he noted, "we all have to keep pushing."

> **"We need to keep engaging with different types of organizations so that they can use CTA's data and tools to fight cybercrime."**
>
> **Ken Xie**
> CEO, Fortinet

With this milestone in the books, everyone at CTA can now look forward to keeping on pushing for many years to come. Be sure to keep an eye on our **website**, **Twitter feed**, and **LinkedIn** for the latest updates on CTA's activities and membership.

SPOTLIGHT: WOMEN OF CTA

Every year on March 8th, the world celebrates International Women's Day. CTA has many fantastic women working with us. Below, we are honored to profile six of them in celebration of this special day. These women each interact with CTA in unique ways, and all are providing great value to the organization and our mission overall. We hope that you enjoy learning about some of the women who make up the Cyber Threat Alliance.



IMELDA FLORES | HEAD OF SCILABS, SCITUM (CYBERSECURITY DIVISION OF TELMEX)

"Focus on the solution, not the problem."

I was blessed to have the opportunity to start working in cyber threat intelligence (CTI) before almost anybody else in Mexico in the private sector. In 2013, when my boss decided to create Scitum's CTI unit — SciLabs — there were only a few of us involved, so I was given a lot of opportunity to build things from scratch. Our goal was to find threats before the attackers could do damage and serve customers by making sure that they wouldn't have cybersecurity problems that would end up on the front pages of the newspapers. The main challenge that we had to overcome was translating from the broader intelligence community into the specific context of CTI and I'm really proud of the work that we did there.

As Head of SciLabs, I am in charge of the Security Automation team, incident response, and CTI. We also handle cybersecurity monitoring and management. These functions altogether give us visibility both inside of organizations as well as more widely across the threat landscape. This makes it possible for us to seek out really interesting or ideally even game-changing intelligence for our customers. Every day brings a new challenge or a new malicious campaign or a new customer with new issues, and I find my mantra to be especially important in responding to this. It's easy to throw blame around in cybersecurity, but what you need to do is stay focused on the solution. In my free time I also try to read about human emotions, connections, and behaviors. People often forget that even in cybersecurity, we're ultimately still dealing with human beings.

For me, CTA is the best collaborative platform out there in the private sector. I've been involved in other collaborative groups that have members in common with CTA and when those groups ask, "How do we improve?" people often say, "Be more like CTA." CTA's collaborative channels are full of really smart, amazing people; being able to go to people and ask about an early share before it's published generates a lot of value, as does being able to verify analytic conclusions with other members. It can also be difficult for others to see what we see in Mexico and Latin America, so when we spot something that we can then share through CTA, everyone benefits.

My advice for women looking to get into cybersecurity is to remember that gender shouldn't matter. Maybe it's because of my background, being the only woman in a family with five brothers who always treated me just like one of them. When I moved into the professional world, I tried to be proactive and generate as much value as I could. Don't second guess yourself; just go ahead and do your thing!

KATE HOLSEBERG | DIRECTOR OF PROGRAMS & MEMBERSHIP, CTA

"It's kind of fun to do the impossible."

My work as Director of Programs and Membership at CTA has brought so much variety. Since taking on that role when I joined the organization in 2017, I've had many opportunities to meet new people and interact with different companies from all over the world. CTA is a globally-focused organization with member companies headquartered across the world, and our recruitment efforts are very diverse. Between connecting with current members and potential members, it is not uncommon for us to one day be talking with someone in Brazil, then the next we're talking to someone in Europe, and then Australia. Particularly as more people have been staying home over the last year, it's been neat to be able to talk to people all over the world and hear what they're doing differently within their niches and their piece of the cyber security pie.

I fully believe in CTA's mission, which is reaffirmed every time we bring on a new member to CTA. Each new member that joins the Alliance broadens our reach, and enables all of us to help expand the protections that members can provide just a little bit further to protect more customers and more of the digital ecosystem. It's a ripple effect. Whether they are CTA members or not, CTA's work has an impact, because having greater security for some also means greater security for everybody. CTA is making an impact not only within the industry, but in people's everyday lives, whether they know it or not. It's a great feeling to be a part of this mission.

CTA just recently celebrated its fourth birthday, and I think that's a pretty great accomplishment in and of itself. As our CEO likes to say, threat sharing is easy to talk about, but hard to do. It's even harder to do at speed and at scale, with high quality data, and in the face of competition. Yet, here we are, four years later with more than five times as many members as when we started, proving that it is possible, and sustainable. I'm a Disney kid at heart and one of my favorite quotes is, "It's kind of fun to do the impossible." In the case of CTA, I agree, Walt.

Beyond CTA, I enjoy getting outside with my family and seeing the world through the eyes of my children. I also enjoy traveling and look forward to being able to connect in-person again with CTA members and the many individuals we meet through our work who are interested in furthering CTA's mission, for the greater good.

KATHI WHITBEY | PROGRAM MANAGER, UNIT 42, PALO ALTO NETWORKS

"The courage to start, strength to endure, and resolve to finish."

I just celebrated 5 years with Palo Alto Networks (PAN) after having spent years in US government contracts developing custom software. I don't think I'd even been with PAN for a month when our CSO called me into his office and said, "I've got a program and I need your help. Can you come with me to California for this inaugural board of directors meeting for CTA?" I remember that first meeting and I couldn't believe it; I was in awe of the people, skills, and knowledge in the room. Some of the biggest badasses in cybersecurity were in this one room, and I actually got to be there with them! At that point we were building out the original CTA sharing platform. I consider myself extremely lucky that our CSO had confidence in me and a willingness to let me grow in that role and take these responsibilities head on.

So, it really just kicked off from there, and now I can smile and say, "Look how far we've come!" I couldn't have imagined that we'd be where we are today when I started with the organization five years ago. I really believe in the mission and think it's important that we continue to collaborate and share, and actually build those relationships. I feel a sense of pride to see the successes that we've had and that's one of the things that really motivates me to continue supporting CTA. The quote above is on a bracelet that I got when I ran my first marathon. It applies in almost everything I do; the courage to get going, the strength to continue, and the resolve to see it through. As long as CTA continues to see these successes, continues to grow, and continues to have great people within the organization itself, I can keep smiling!

To be successful also means to have a well-balanced life. I have been very lucky to be able to travel the world for work and to spend time taking care of me through running and racing, as well as spending hours giving back to my community through volunteer work. For example, in 2010, I started volunteering as an EMT and I was actually able to take a year off my career to go to Djibouti to support the U.S. Navy with their fire and rescue department. It was really a neat experience and I got a lot out of supporting the military that way, and especially in a foreign country. I've volunteered with Girl Scouts for over 15 years now. I've run marathons and half marathons on four continents, including Antarctica. And I continue to volunteer as an EMT supporting local organizations.

There are a lot of things that I'm proud of from my career. From creating incredibly specific and complicated software programs, to traveling the world to deploy new programs and teach end users how to be successful. But CTA is at the top of my list of things that I'm proud of in my career. I will talk to anybody, anytime, anywhere about CTA.

SARA EBERLE | HEAD OF GLOBAL PUBLIC RELATIONS, SOPHOS

"Only positive chain reactions."

Will what I'm going to do today have positive chain reactions on the world, on CTA, my work colleagues, or Sophos overall? Everything we do has ripple effects, and I always want these effects to have positive chain reactions. This is my mantra in life.

I was starting my career when the Morris worm came out and I remember being intrigued by it. Little did I know that I would soon be working in cybersecurity with Symantec, one of my clients in the 1990s when I had my PR firm in Los Angeles. My agency helped launch numerous tech industry firsts, such as the Diamond Rio, and we did groundbreaking press work, including handling TV and other media communications for threats like the Melissa virus and Love Bug. I remember being on a cybercrime media tour in Washington, D.C., flying home to Los Angeles, landing, hearing about Love Bug, getting a call from NBC's Today Show, and then hopping back on a plane to New York for an interview with Symantec's spokesperson. We racked up a lot of frequent flier miles that week. Fast forward to 2016. I started working at Sophos, bringing with me a unique perspective on how to talk about cyber threats with the media. I was on the frontlines with the press when cybersecurity was just taking off as an industry and I had 30 years of PR and journalism experience. With this background, I'm able to develop media strategies for communicating diverse, often complex, issues and news topics to optimally impact Sophos, the cybersecurity industry, and CTA.

At Sophos, I work closely with our threat hunters and SophosLabs threat researchers. Hearing about changing attacker behaviors and the different ways we can stop them is fascinating. Every day the PR team learns something different about what's happening in the world of cybercrime and why organizations need certain protection and defenses. Because we have direct access to information from our threat intelligence experts, we can quickly determine relevant news content and figure out what parts will be interesting to journalists — and that's one reason why I've been successful in PR. I know how to take on a journalist's viewpoint. With the resulting press coverage, defenders can learn more about the latest attacks and improve their security.

Cyber attackers are well-coordinated, so security vendors should be as well. If we have one piece of the puzzle that another vendor doesn't have, which they need to provide better defenses, then we should be coming together to share intelligence. The mission, vision, and collaborative philosophy of CTA are critical. I like when CTA's communications committee embraces this philosophy. We are stronger when we share ideas and challenges the way the threat intelligence experts do.

When I am not at work, I spend my time with my husband and teenagers. We have a large backyard with a garden where I grow heirloom tomatoes. Even though we harvest a lot of fruit, it's not enough for my annual canning project, which requires about one-hundred pounds of Roma tomatoes. These I buy from a local commercial farm. I learned how to can from my Italian-American grandmother, who "put-up" everything in sight in the 1970s. My grandmother also taught me to cook and inspired me to write a cookbook. My co-author and I just self-published our first cookbook a few weeks ago. It's the first in a series we have already written and plan to publish over time. Right now, we have our hands full with our careers and families, so launching one cookbook is plenty enough.

JEN MILLER-OSBORN | DEPUTY DIRECTOR OF THREAT INTELLIGENCE, UNIT 42, PALO ALTO NETWORKS

"Be afraid, but do it anyway."

I got my start in cybersecurity twenty years ago while on active duty in the Air Force. The government was starting to get into information security and cybersecurity and, since there wasn't a workforce for it initially, they looked to people who had similar or useful skillsets. They asked me if I wanted to volunteer for a pilot program that they were going to be running; I liked computers and I liked languages, so I thought it sounded like fun. If nothing else, it was going to be different from my day-to-day., and it's turned out to be a lot of fun!

Palo Alto Networks (PAN) is my first foray into the private sector side of cybersecurity — all of my experience before that was with some version of government or law enforcement, including at MITRE where I was one of the founders of the ATT&CK framework. I and my team handle everything outward facing for Unit 42; all of our global outreach, analytical partnerships, blogs, social media, and white papers as well as our government and law enforcement engagement. We work directly with organizations that can make a real-world difference in stopping malicious cyber activity, which also includes ensuring that we're sharing threat intelligence as broadly as we can.

From my perspective, one of the things that really hamstrings a lot of government work is that it's so restricted in terms of who you can talk to, what you can share, and who you can work with. I really appreciate the freedom that I have in my role at PAN to share threat intelligence and work more freely across the industry with access to broader datasets and different mindsets. At this point in my career as I'm shifting back into management, I also really enjoy encouraging and mentoring my teammates, and seeing them grow our government programs, our law enforcement partnerships, and all of our work with CTA as well. It's awesome to see what we've been able to do over the past couple of years in those areas.

I'm especially proud of the work we do with the CTA's Early Sharing Program. I started sharing our blogs with CTA at the same time that we send them out to people who are on our Trusted Information Partner Sharing (TIPS) list, and still send them to this day. CTA's A&I Committee is also one of the more active communities in this space, even offline, in terms of reaching out and sharing. It's a win-win situation all around.

On a personal front, my husband and I have four rescue dogs and two cats. We spend a lot of time playing with them outside. The oldest is a Standard Poodle named Mobeus. Then we have Maggie, who is a ridiculously cute Golden Retriever-Bassett mix, then we have a little Pitty-lab mix, and then over the pandemic we took in a litter — and we foster-failed on one of those, which we think might be a Boxer-Great Dane mix. He's just a goofball. They keep us busy that's for sure!

SHEBA GRACE | VICE PRESIDENT, K7 COMPUTING

"Never, ever give up."

I've been at K7 for my full 26 years in cybersecurity, but before that I worked in marketing for a leading Indian IT magazine. I had actually done a technical diploma in computing but since I was pretty talkative people suggested that marketing was a better fit for me than coding.

One day, I visited K7 to sell them advertising space in the magazine. By accident I peeked at one of the computers, and noticed that they were coding in C and asked some questions from the lines of code I was able to see, which gave away the fact that I had some technical background. They offered me a job that same day, and since any challenge is appealing to me, I naturally took it! Since then, I've been able to take on a lot of different responsibilities. Now, I'm largely in a management role handling the internal operations of K7.

Back in the early days, it was extremely difficult as a small Indian company to get access to malware samples. K7 wasn't widely known in the industry, so it was difficult to build the relationships and trust needed for information exchange with larger vendors. Part of my job was to build relationships within the industry, including industry veterans, and explain what K7 did and how our collaborations could be mutually beneficial. That's a big part of how we grew. And having come across these initial hurdles with the help of our industry friends, K7 decided we should be giving back to the industry as much as we can. This is a major reason why K7 contributes heavily to the Association of Antivirus Asia Researchers (AVAR).

These days, cybersecurity is very different; we all fight on the business end but collaborate really well on the technical front. The internet has obviously helped with that, but there's still a lot of value in creating relationships and having platforms where people can interact with each other.

I think CTA is doing a fantastic job on those aspects, and K7's relationship with CTA is also important since it helps us place the quality of our intelligence in a global context. If each company is going to look only at the threat landscape of the regions in which they are present and just keep their research to themselves, then fighting the bad guys is going to be much harder. Today, the core essence of protecting your customers is having access to global threat intelligence and CTA is doing an excellent job helping companies share that information. CTA is also very open and direct in working with its members, understanding their needs and supporting them as much as possible.

For fun, I love spending time with my children. They're 15 years old and 8 years old. My daughter loves TV shows and movies, so I'll sit with her and watch whatever she's interested in at the time, while my son and I both love the beach, which is only a fifteen-minute drive from where we live. My husband and I have both worked at K7 for a long time, so we're blessed that our kids have always been easygoing around our work responsibilities. They even travel with us to almost all the security conferences! There has been a joke that my daughter should probably get VirusBulletin's 10-year badge given to regular attendees of their annual conference.