JUNE 2023

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

One common logical fallacy is called the appeal to nature. This fallacy relies on the assumption that things are the way they are because it is "natural." That assumption often proves false in the physical world, and it almost always proves false in cyberspace. Usually, things are the way they are because of decisions we have made, either individually or collectively as societies. Yet, we often accept these decisions as the way of the world and fail to challenge them, even when they generate poor outcomes for most individuals.

We face this situation in cybersecurity. We take it for granted that end-users, whether individuals, small businesses, or giant corporations, are responsible for the entirety of their cybersecurity. We accept the idea that software comes with known vulnerabilities and that the core functions of the Internet are insecure. Yet, these outcomes stem from policy decisions about the software market or how to operate the Internet, not due to the laws of nature. We could make different policy choices in all of these areas.

The recently released US National Cybersecurity Strategy makes the case for such a change. It argues for shifting a large portion of the security burden away from end-users to the entities most capable of handling it. As the strategy states, relying on every individual or small business to have good cybersecurity all the time is not an effective approach over the long-term. Instead, the Strategy lays out a different set of policy choices that would alter the status quo and change the distribution of the security burden in the US digital ecosystem.

Changes of this magnitude do not happen overnight or without a lot of debate. Yet, logically, we must change how we approach cybersecurity if we want a better outcome. The debate should be around how to achieve such an outcome. How should the burden be shifted? Who takes on additional responsibilities? What protections or support should we provide for those entities taking on more responsibility? What guardrails or oversight mechanisms do we want to put in place? How do we maintain innovation?

In this newsletter, CTA members and partners explore the concept of burden shifting. You will find a wide variety of recommendations and approaches. That's a good thing, because we are only at the very beginning of this long-term effort, and we need as many ideas as we can get. I am looking forward to these discussions.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CTA WELCOMES NEW BOARD DIRECTORS

We are pleased to announce that Dave Beabout, Global CISO, NTT Security Holdings, and Samantha Madrid, Group Vice President, Security Business & Strategy, Juniper Networks, have been elected as Affiliate Directors to the CTA's Board of Directors for a two-year term. We also welcome Michael Sikorski, VP & CTO, Unit 42, Palo Alto Networks, as the new board member representing CTA Charter member Palo Alto Networks.

"I am very happy to welcome Mike and Dave to the CTA board. They will bring a wealth of insight from their time in the cybersecurity industry," said Michael Daniel, President and CEO of CTA. "I am also pleased to have Samantha continue her service on the CTA board. Her questions, feedback, and oversight have helped make CTA stronger as an organization."

We would like to extend a huge thank you to our out-going board director, John Petrie, Counselor to the NTT Global CISO and the Liaison for NTT Ltd. John's contributions to CTA have been invaluable and we greatly appreciate his dedication to CTA.

Dave Beabout
Global CISO,
NTT Security Holdings

Samantha Madrid
Group Vice President,
Security Business & Strategy,
Juniper Networks

Michael Sikorski
VP & CTO, Unit 42,
Palo Alto Networks

John Petrie
Counselor to the NTT Global CISO and
the Liaison for NTT Ltd.

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>10 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	35%
IP ADDRESS	18%
DOMAIN NAME	4%
URL	3%
NETWORK TRAFFIC	32%
FILE PROPERTIES	7%
HOST	1%

TOTAL EARLY SHARES

3-5
PER WEEK

825+

CTA Member Feature

RESPONSE TO SHIFTING THE BURDEN

BY LYNDA GRINDSTAFF
VICE PRESIDENT
MCAFEE

Since 2021, McAfee has been a pure-play consumer company, and, as a result, our perspective on this topic is unique. Our customers are often not able to prepare for or prevent cyber-attacks, but they are very much impacted by the downstream effects of these events, whether it's through identity theft enabled by data breaches, supply chain disruption, or loss of access to everyday tools or applications. The burden of protecting data and even finances often fall on them. Yes, the breached corporation or organization frequently provides free resources, such as credit monitoring, to mitigate the impact, but often by that time, the damage is done.

Our world is primarily digital and wholly reliant on the continuous operation and availability of connected critical infrastructure. This massive threat landscape, combined with the pace of technology innovation and the drive of cyber criminals and nation states, means that we are in a constant race to essentially secure the American way of life. While we can never promise that there will be no cybersecurity events, we can do more to prevent and guard against these attacks.

By incentivizing organizations to invest in cybersecurity and resilience, The National Cybersecurity Strategy released by the Biden-Harris Administration in March of 2023, encourages preparedness and a shifting of the burden of these attacks away from individuals, small businesses, and local governments – three groups that are not typically equipped to respond to these events.

This is a step in the right direction, but it's one step in what we should look at as a marathon, not a sprint. Our digital infrastructure was built over a span of decades, and often consists of networks, applications and tools that are inextricably interwoven. This isn't an issue that can be solved in silos or by any single entity.

What IS needed? Innovative and enhanced collaboration between companies and organizations providing software, tools, and infrastructure. We have normalized this on the incident response side, banding together to fight cyberattacks once they are discovered, but we also need to continue to improve these ties and strengthen these connections with an aim of preventing these attacks.

CTA Member Feature

SHIFTING THE SECURITY BURDEN

BY JOE CHEN
VP ENGINEERING
SYMANTEC, DIV OF BROADCOM

Securing the global digital ecosystem against ever-growing threats is a challenge that depends on collaboration. The Cyber Threat Alliance brings together a diverse group of organizations, fostering information sharing and joint efforts to tackle threats. By building trust and sharing resources and expertise, members can achieve far more than they could individually, ultimately spreading the security burden onto the collective shoulders of the alliance to help our mutual customers.

While traditional threat intelligence typically comes days, weeks, or months after it is discovered, CTA drives real-time sharing. Members regularly exchange millions of indicators of compromise with valuable context on an automated platform. More critically, though, is the sharing of research before it is released to the public. We've seen over 800 of these early shares since the program began a few years back. Getting access to new, deployable threat intelligence allows us to enable proactive defense measures. At Symantec, a Division of Broadcom, around 50% of early shares result in us adding new protections, and the other 50% allow us to validate existing protections. Sharing allows members, big and small, to gain a more comprehensive view of cyber threats than any one company could on their own.

Along with real-time and automated sharing, our team has a network of peers in the CTA, built on trust. Member companies are ready to coordinate responses and share resources during times of crisis, which is paramount in defeating attackers. This level of collaboration ensures faster and more effective protections, reducing the impact of cyber incidents and protecting critical infrastructure.

As a founding member of CTA and one of the largest industry threat intelligence contributors, we at Symantec also use our role in the alliance to better the cybersecurity community by collaborating with other members through thought leadership. We continue to value and support CTA's mission, so It makes sense to share our thoughts and spread the word at industry conferences and events. We hope to see even more organizations in our industry join the effort. Only when the cyber industry works together can we improve cybersecurity for all.

CTA Partner Feature

SHIFTING THE SECURITY BURDEN

One of the key proposals in the U.S. National Cybersecurity Strategy is to shift the burden of addressing cyber-insecurity from the less sophisticated to more capable actors – software companies, infrastructure providers, etc. "Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens." Strategy, p.4.

Asking more capable actors to carry the burden of protecting others is the right path. The Global Cyber Alliance has been working to extend cybersecurity to everyone for eight years. We have found that smaller organizations and people struggle not only with resources, but with the basic understanding of what actions to take.

To shift the burden, the Strategy proposes liability for the producers of insecure software. The Strategy takes a smart approach by proposing a liability "safe harbor" for those who follow development best practices. That is exactly the right thing to do: lead with the carrot by asking people to do what we know works regarding secure development and offering them a benefit to do that. Beyond a safe harbor, however, the devil is in the details. The unintended consequences of unclear liability rules could dash innovation in the software ecosystem and put smaller companies and individual developers at a significant disadvantage. The consequences for open source could be huge. So it's better to start with a safe harbor incentive instead of new liability rules, and see where that takes us.

In order to remove the burden from people and small organizations, efforts to proactively secure the Internet itself are even more critical than introducing liability rules. Everyone relies on a safe, available and secure Internet, and the stronger the Internet is, the fewer security issues people will need to take care of themselves. Unfortunately, the National Strategy only touches upon this need in "Secure the Technical Foundations of the Internet." This section contains only two paragraphs, but includes the most important sentence in the entire Strategy: "The Federal Government will ... partner[] with stakeholders to develop and drive adoption of solutions that will improve the security of the Internet ecosystem and support research to understand and address reasons for slow adoption." P. 24. This is also exactly right, but how will this be accomplished? Partnering to develop and drive solutions to secure the technical foundations of the Internet will do more than any other action to shift security burdens away from the most vulnerable small businesses and individual citizens.

BY PHILIP REITINGER
PRESIDENT AND CEO
GLOBAL CYBER ALLIANCE

CTA Member Feature

US NATIONAL SECURITY STRATEGY: SHIFTING THE BURDEN

NTT

The Biden-Harris Administration's recent release of the National Cybersecurity Strategy is a significant milestone in our collective efforts to secure a safe and resilient digital ecosystem. This strategy has the potential to reshape the cybersecurity landscape, and it is essential for everyone to understand its implications and how it can impact our daily lives.

The strategy outlines a vision to reimagine cyberspace as a tool to achieve national goals while reflecting core values such as economic security, human rights, trust in democracy, and an equitable society. It proposes a fundamental shift in the allocation of roles, responsibilities, and resources, focusing on rebalancing the responsibility of defending cyberspace. This approach aims to shift the cybersecurity burden away from individuals, small businesses, and local governments; placing it onto organizations that are better equipped to reduce risks for everyone. This is important as the Biden-Harris Administration has made it clear the intent of this strategy is to improve digital security everywhere and as a result improve the lives of U.S. citizens.

What is also important here is the shift of burden will come with an assumed increase in regulatory oversight and we do not yet have clarity on the impact this will have on those to whom the burden has shifted. This shift will no doubt have a second and third order impact on regulatory guidance adopted in other like-minded countries. Security leaders and Chief Information Security Officer's (CISO) with international operations will need to keep an eye on how this unfolds in the next three to five years.

From a CISO's perspective, there are several key takeaways from this strategy that can directly influence our daily lives:

- Enhanced Collaboration: The strategy encourages collaboration between the public and private sectors to defend critical infrastructure and essential services. This focus fosters a more efficient and rapid response to cybersecurity challenges, ultimately enhancing the security of our digital ecosystem. It presents an opportunity for everyone to benefit from a collective defense and enjoy a safer online environment. This is also where CTA has the potential to have a huge impact due to its role, membership, and the voice it has back to the security community.
- Long-term Investment Incentives: The strategy promotes striking a balance between addressing urgent threats and investing in a resilient future. This approach aligns with the need to ensure that cybersecurity investments made by organizations and governments are strategically planned allowing us to stay ahead of evolving threats and mitigate risks effectively.
- Focus on Critical Infrastructure: The strategy prioritizes defending critical infrastructure, which is essential for the smooth functioning of our society. As more aspects of our lives become dependent on technology, ensuring the protection and resilience of critical assets is crucial for everyone's safety and well-being.
- Emphasis on Workforce Development: The strategy highlights the need for a diverse and robust national cyber workforce. This focus is vital for creating a skilled pool of cybersecurity professionals who can effectively manage the evolving threat landscape, ultimately making the digital world safer for all of us.

However, the strategy also presents challenges that we must address as a society:

- Implementation Challenges: Ensuring the strategy's successful implementation may require significant effort and resources from governments, organizations, and individuals. It will be crucial for everyone to stay adaptable and responsive to the changing cybersecurity landscape while effectively allocating resources to meet these new requirements.
- Balancing Privacy and Security: With the strategy's emphasis on privacy and personal data security, we must strike a delicate balance between protecting individuals' privacy and sharing information to improve our collective cybersecurity efforts.
- Legal and Regulatory Challenges: Implementing the strategy may lead to new legal and regulatory complexities, particularly around data privacy, cross-border data sharing, and liability concerns. Navigating these complexities will be essential for maintaining an effective cybersecurity program and a safe digital environment.

In conclusion, the National Cybersecurity Strategy presents both opportunities and challenges for everyone. By understanding and embracing the strategy's objectives, we can contribute to building a more secure and resilient digital ecosystem for ourselves and future generations.

BY DAVID BEABOUT
CISO
NTT SECURITY HOLDINGS INC.

THANK YOU, CRAIG!

The CTA is pleased to announce the approval of a generous grant from Craig Newmark Philanthropies supporting our CTA mission to raise the level of cybersecurity across the digital ecosystem. The funds will be used to create joint reports on cyber threats and mitigation, combining the knowledge of CTA members and partners.

"I am very pleased that Craig Newmark Philanthropies has decided to support CTA's mission," said Michael Daniel, President and Chief Executive Officer of CTA. "We will use the funds to work with our members and partner organizations to identify under-reported cyber threats, provide information about those threats, and lay out how to mitigate them. Strong philanthropic support enables organizations to pursue activities that benefit society broadly, including cybersecurity. Craig is a leader in this area, and I hope that others will follow to expand the amount of funding available for these kinds of public missions."

Craig's overall support for improving the protection of the internet is impressive and his generosity in supporting the CTA mission is much appreciated.

craig newmark philanthropies

CTA Member Profile

MEMBER SPOTLIGHT: NETSCOUT

NETSCOUT®

WHY DID NETSCOUT JOIN CTA?

I had been aware of the CTA since its inception and had the opportunity to see it mature, from afar. As we were thinking through our outreach and engagement here at NETSCOUT ASERT, we recognized the value of joining our peers in CTA. Our objective at the outset was to focus on the threat content sharing, but we soon realized that there were many other aspects to our participation that justified the endeavor.

WHAT DOES NETSCOUT VALUE MOST ABOUT CTA MEMBERSHIP?

We find the ability to collaborate with our peers is the most valuable benefit. It helps to see the research up front and gives us the ability to conduct dialogue about breaking threats, have conversations about tradecraft, and jointly work on issues where we're clearly coming at things from different angles.

HOW DOES BEING PART OF CTA HELP NETSCOUT PROVIDE GREATER SECURITY FOR CUSTOMERS?

Our customers rely on us to understand the broader threat environment, and even as we have our own research and methods of acquiring the data underlying our findings, we benefit greatly from the perspective that our CTA partners bring. This can help overcome biases that naturally occur for various reasons, including where we instrument and analyze. Our customers need us to stay informed, and we get to reach beyond our typical cone of visibility thanks to the engagement with the CTA.

WHAT VALUE DOES NETSCOUT GAIN FROM PARTICIPATING IN THE VARIOUS WORKING GROUPS THAT FOCUS ON SPECIFIC THREAT CAMPAIGNS OR SPECIFIC EVENTS, LIKE THE OLYMPICS OR ELECTIONS?

We have a strong focus on DDoS here at NETSCOUT ASERT and this results in a strong complementary view during large scale events, where the intrusions and the DDoS attacks often go hand-in-hand. We believe that few can speak about DDoS events like we can, but we recognize that this is just part of the threat spectrum that is observed during say, an election, or at the start of a major war such as the invasion of Ukraine. The Working Groups are an excellent forum for us to compare notes with our colleagues and it's even better when the CTA facilitates access to the stakeholders who might range beyond our core customers.

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

It might be that I'm a little jaded, but the challenges haven't changed all that much from my point of view. Numerous adversaries with differing motivations and capabilities remain interested in access and denial to infrastructures that we rely on to conduct normal life and business activities, and it so happens that these infrastructures are evolving in ways that introduce new fragilities and modes of exploitation. Within these constructs, lots of things have changed over the past few years, and I figure much will change going forward. I'm personally fascinated by the fragmentation of the cybercrime domain and our inability to impose structures on them. I have no doubt that the collective nature of the CTA will be key to the progress that we make in protecting society against the evolution.

IN CLOSING, IS THERE ANYTHING YOU WOULD LIKE TO LEAVE US WITH?

We at NETSCOUT are proud supporters of the CTA and celebrate the progress that has been made during the time it's been operating. We look forward to being contributors in the years to come.

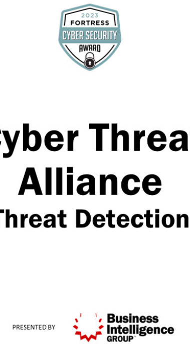
BY HARDIK MODI
AVP ENGINEERING, THREAT AND
MITIGATION PRODUCTS AT NETSCOUT

CTA in the News

FORTRESS CYBER SECURITY AWARD

The Business Intelligence Group presented the Cyber Threat Alliance with the 2023 Fortress Cyber Security Award in the threat detection category. The industry awards program identifies and rewards the world's leading companies and products that are working to keep our data and electronic assets safe among a growing threat from hackers. CTA is proud of our members working together to better protect their customers and the digital ecosystem.

"We are so proud to name the Cyber Threat Alliance as a winner in the 2023 Fortress Cyber Security Awards program," said Maria Jimenez, Chief Nominations Officer, Business Intelligence Group. "As our society continues to evolve and become more reliant on networks and data, companies like the Cyber Threat Alliance are critical at providing the protection and trust consumers demand."



2023 FORTRESS CYBER SECURITY AWARD

Cyber Threat Alliance
Threat Detection

PRESENTED BY Business Intelligence GROUP

Upcoming Events

JOIN US AT VIRUS BULLETIN 2023

The Cyber Threat Alliance is proud to sponsor the Virus Bulletin Conference Threat Intelligence Practitioners' Summit (TIPS) again this year. The conference will take place in London, UK and runs Oct 4-6th with the TIPS track on Oct 5th.

The theme for the TIPS track is 'The Community Effect'. Check out the program here.

REGISTER HERE