House Committee on Homeland Security

"A Borderless Battle: Defending Against Cyber Threats"

Written Testimony of:

Michael Daniel

President, Cyber Threat Alliance

March 22, 2017, 10:00 a.m.

House Capitol Visitor Center – Room 210

Chairman McCaul, Ranking Member Thompson and Members of the Committee:

Thank you for the opportunity to appear before you today to discuss how new models of collaboration and threat sharing can be a catalyst towards tangibly reducing threats across the cybersecurity ecosystem. My name is Michael Daniel and, as of last Monday, I am the first President of the Cyber Threat Alliance (CTA)—a cyber threat information sharing organization that now includes six of the world's largest cybersecurity companies as founding members. Prior to leading the CTA, I served for over 20 years in the U.S. federal government, most recently for four years as Special Assistant to the President and Cybersecurity Coordinator at the National Security Council.

First, let me begin my testimony by acknowledging this Committee's longstanding leadership on cybersecurity issues. This Committee has played a central role in passing a range of important cybersecurity legislation, including legislation that has helped foster a more robust and trusted environment for responsible cyber threat information sharing. Having worked on cyber threat information sharing issues firsthand for many years, I understand how challenging this process was and sincerely appreciate this Committee's continued hard work and leadership.

The Cyber Threat Landscape

We live in a digital age. This digital age brings with it incredible efficiencies and productivity, but it also brings new challenges and potential vulnerabilities that—left unchecked—threaten to undermine these very benefits. The increasingly digitized nature of the world, and the United States in particular, means the threats we face in cyberspace are particularly significant. Our economy, our national security, our social lives all depend heavily on the Internet and cyberspace. Unfortunately, the threat is also growing more acute in at least three fundamental ways:

1) The cyber threat is becoming broader: As we increasingly connect more and more devices up to the Internet, we are making cyberspace bigger and dramatically expanding the potential attack surface. Indeed, even by the Gartner Group's conservative estimates, there will be over 20 billion devices connected to the Internet by 2020—that translates to adding 10 million devices per day. But more important than just the numbers are the kind of devices we are connecting to the Internet. They are not desktops, laptops, or even smartphones. They are light bulbs, refrigerators, cars, thermostats, sensors, and thousands of other "things"—a huge array of different kinds of devices with different functions, protocols, and security features. This growth in volume and heterogeneity makes effective cyber defense even harder.

2) The cyber threat is becoming more frequent: The number of malicious actors in cyberspace continues to grow rapidly as hacktivists, criminals, and nation-states all learn that they can pursue their goals relatively cheaply and effectively through cyberspace.

The barriers to entry are low and the potential return on investment is fairly high. As a result, the volume and frequency of malicious cyber activity is increasing dramatically.

3) The cyber threat is becoming more dangerous: Until recently, cyber actors generally limited their malicious activities to stealing money or information, temporary denial of service attacks, or website defacements (the digital equivalent of graffiti). But increasingly, we are now seeing actors move to much more destructive and disruptive activities. The destructive cyber attack on Sony Pictures Entertainment, the physical disruption of the Ukrainian power grid, and the use of information operations to influence electoral processes are all recent examples of this trend.

Why is cybersecurity a hard challenge to solve?

At first glance, it's not obvious why cyber threats are so hard to effectively manage. If it's just a technology problem, why can't we simply deploy innovative technical solutions to stop these threats? The answer is that cyber threats pose not just technical problems, but also economic, psychological, and human behavioral challenges. As a result, our response to threats has to involve not just technical solutions, but economic, psychological, and human behavioral aspects as well—a much greater challenge than simply buying a new cybersecurity device or service.

In addition, cyberspace operates according to different rules than the physical world. I do not mean the social "rules" of cyberspace that get a lot of play in the media, but rather the physics and math of cyberspace. The concepts of distance, borders, proximity – all operate differently in cyberspace compared to the physical world. Therefore, our typical models for addressing certain challenges, such as border security, simply don't work in cyberspace. Developing these new models will take time and experimentation to get right.

Finally, cyberspace and the Internet are still very new, relatively speaking. From a policy and legal perspective, we have not had the time or the experience to develop the comprehensive frameworks we need to tackle cybersecurity's challenges. What is the right division of responsibility between governments and the private sector in terms of cyber defense? What actions are acceptable for governments, companies, and individuals to take and which actions are not? Answering these kinds of questions is the fundamental policy challenge for the next few years.

What should we do about cybersecurity?

Given the trends, growing complexities, and inherent challenges of the cyber threat, is it possible to design an effective strategy to combat it? The short answer is yes – but implementing such a strategy requires a lot of work, sustained engagement, and a multi-disciplinary, risk-based approach. As a nation, an effective cyber strategy will involve three core elements:

- Raising the level of cybersecurity across the global digital ecosystem
- Preventing, disrupting, deterring, and constraining our adversaries' operations in cyberspace
- Responding effectively to incidents when they occur

From an organizational perspective, an effective cyber strategy must also contain several core elements:

- Making cybersecurity a C-suite and organizational priority
- Using a risk-based approach to address cyber threats
- Developing, testing, and exercising an incident response and recovery plan

In developing their strategies to combat cyber threats, governments should recognize that no one agency has the full range of capabilities, authorities, and perspective needed to address the challenge. Organizations must realize that they cannot relegate cybersecurity to the Chief Information Officer's (CIO) shop or the geeks in the server closet. Collectively, we must realize no government or individual company can effectively address the cyber threat by itself. Instead, cybersecurity is a fundamentally shared and distributed challenge that can only be effectively addressed through collaboration that leverages the unique capabilities and authorities of companies, individuals, and governments. The private sector, state and local governments, national governments – all of these entities will have to work together across boundaries and borders if we want our cybersecurity strategies to be effective.

In considering how to build this new kind of collaboration, I don't have "the" solution for what it should look like. In fact, there's almost certainly not just one solution. However, through the hard work of many people over the past decade and a half, we have started building the foundations for this new kind of collaboration. This Committee has passed critical legislation that enables this collaboration within the U.S. The Federal government has worked hard to build its capabilities across all the relevant agencies – Homeland Security, Defense, Commerce, State, Justice, GSA, OMB, and the Intelligence Community all have critical roles to play within the U.S. context. This kind of interagency collaboration will be necessary in other countries as well. The private sector has also been working hard globally, creating new structures, like Information Sharing and Analysis Organizations, building new technologies, and creating whole new industries, like cyber incident response firms. So the good news is that we do not need to start over. Instead, we can continue building on this foundation laid over the last decade to evolve this collaboration into its effective form.

Cyber threat information sharing as a critical component of effective cybersecurity

Clearly, if we are going to have the kind of interagency, intercompany, and interorganizational collaboration I described above, cyber threat information sharing is a critical enabler. In fact, robust cyber threat information sharing across this entire cybersecurity ecosystem is a necessity in achieving our shared goals of enhanced cybersecurity. Of course, cyber threat information sharing won't solve the problem by itself. If it is not used as a tool to leverage people, process, and technology to match the highly automated nature of our adversaries' attacks with automated defenses, then it will not be effective.

Despite this obvious enabling function, as a society we've had trouble figuring out how to actually share useful cyber threat information, do so at a speed that matters, and then to take action based on that information. That's where the CTA comes in.

How does CTA help achieve these goals of automated defense?

Within the cyber threat information sharing environment, cybersecurity companies have a unique role to play. They collectively have the physical infrastructure and processing ability to automatically deploy preventive measures based on new cyber threat information to a broad customer base across multiple sectors. For these reasons, cybersecurity companies can bring a degree of "actionability" to cyber threat information sharing that is critical for achieving the ultimate goal of raising adversary costs and tangibly improving cybersecurity across the ecosystem.

To make this potential real, a core group of cybersecurity companies decided to form the Cyber Threat Alliance (CTA). CTA is a new kind of Information Sharing and Analysis Organization (ISAO) that features six of the largest global cybersecurity companies as founding members—Check Point, Cisco, Fortinet, McAfee, Palo Alto Networks and Symantec. It also includes IntSights, Rapid7, Reversing Labs, RSA, and Telefonica as affiliate members. This partnership underscores the philosophy that we can be force multipliers in support of a coordinated cyber threat information sharing effort against our shared cyber adversaries. The CTA cyber threat information sharing model is novel in several ways that directly address many of the aspects that have limited the effectiveness of other cyber threat information sharing relationships, both formal and informal:

1) Accountability- The CTA ensures that there is no anonymity for member contributions, although the customer's data is anonymized. Therefore, submitters have to stand behind the accuracy of the cyber threat information they provide.

2) Participation- To encourage active participation and meaningful contributions, the CTA establishes mandatory submission thresholds for cyber threat information sharing, initially on a quantitative basis in an ever evolving scoring system that measures the qualitative value of shared cyber threat data based on context.

3) Transparency- The CTA uses an automated scoring algorithm to evaluate and assign point totals of submitted cyber threat intelligence that will be public among all members. CTA members will all be able to measure their performance on a dashboard.

Using this new cyber threat sharing model, CTA undertakes two broad operational lines of effort. First, CTA enables near-real time sharing of rich, contextual cyber threat information among all cybersecurity companies, which can be leveraged on an individual basis to update and improve their products and services. Second, CTA uses this shared cyber threat information to build "playbooks" of malicious cyber activity. Taken together, these two broad lines of effort enable CTA to support both national and organizational cybersecurity objectives, including:

1. Improved cyber defense across the entire ecosystem– By enabling cybersecurity providers to dramatically expand the pool of information their defensive products can leverage, every member's products become more effective for their customers. Because the CTA members' customers span all industry sectors, the impact of this cyber threat information sharing can protect a larger percentage of the global ecosystem than more sector-specific information sharing entities.

2. Better prevention against, and disruption of our adversaries– The CTA is focused on sharing indicators related to an adversary's playbook – a more limited and predictable series of steps an adversary must take to complete a successful cyberattack. Although re-engineering malware requires some time and effort, relatively speaking it is easy to make small tweaks to malware so that it can evade detection. However, an adversaries' total suite of indicators (the "playbook," including tactics, techniques, and procedures, and typical operational approach) is much more difficult to change and update. By developing and publishing these playbooks, we can force adversaries to adapt their business processes – a much more time consuming and therefore disruptive task.

3. Risk-based– As CTA's cyber threat information base grows, it will enable better analysis of cyber threats and trends with respect to those threats. In turn, this analysis will enable our members to better advise clients on the relative risks of the cyber threats they face and how to prioritize among them. This type of broad-based sharing of widely used threat techniques can help neutralize unsophisticated actors and force sophisticated adversaries, such as nation-state actors, to develop new (and therefore costlier) techniques. This narrowing of the threat landscape can enable public and private organizations to more effectively target high-priority and advanced persistent adversaries and threats.

4. Incident response and recovery – CTA cyber threat information sharing will lead to better information, particularly about adversary playbooks, that can make incident response and recovery efforts faster and more effective.

To fulfill these core missions, the CTA has built an automated cyber threat information sharing platform with the goal of enabling and incentivizing the sharing of high-quality, actionable cyber threat information. The CTA and its platform embody a major step forward in transforming shared cyber threat information into effective preventive measures that can automatically be deployed by CTA members to their respective customers. The CTA platform is not just a concept or a set of Powerpoint slides – it is a functioning system, actively working to protect its members and their customers in near-real-time, and thus contributing to the increased protection of the industry and the world.

For example, recently, a single shared cyber threat sample from one CTA member allowed another member to build protections before that organization's customers were targeted – preventing successful attacks against 29 subsequent organizations. In another instance, cyber threat data shared through the CTA from one member allowed another member to identify a targeted attack against its customer and release additional indicators to defend that organization. The CTA and its platform have shown that a well-designed and well-built cyber threat information sharing program can improve the nation's cyber defenses and undermine the efforts of cyberadversaries. CTA is already improving cybersecurity, with some members finding that 40 to 50 percent of CTA's shared cyber threat data is new and directly actionable.

Better cybersecurity

The cyber threats we face as a world are very serious. For over forty years, the United States and other like-minded countries have used the Internet and cyberspace to derive enormous benefits: economic growth, national security improvements, and social well-being. However, if we do not begin to effectively address the cyber threats we face, those benefits could wither. That is not a future we want. Tackling this challenge effectively will require forging new partnerships within industries, between industries, and between the government and industry. It will require organizations to adopt new mindsets and change old beliefs to reflect the realities of the modern cyber threat environment. It will require coordinated action in a manner that reinforces market forces and competition. The Cyber Threat Alliance is ready to do its part in this endeavor and achieve effective cybersecurity for everyone around the world.