NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION

Fighting the Invisible Hurricane—Why a Public-Private Cybersecurity Partnership Supports National Security

By Larry Williams
President
National Technology Security Coalition

President and CEO
Technology Association of Georgia

Board Director, Technology Councils of North America

When the Category 5 Hurricane Michael hit the Southeastern United States in October 2018, a well-honed apparatus began to operate. Florida Governor Rick Scott and Georgia Governor Nathan Deal declared states of emergency. President Trump issued emergency disaster declarations. FEMA offered hazard mitigation and public assistance, and the military supported FEMA's response efforts. A combination of nonprofits, private companies, and volunteers also organized, coordinated with the public sector, and helped.

Visually, we can easily see the devastation from such a storm—the deaths, damage, and disruption. So, if someone said a hurricane was just the private sector's responsibility, we would be horrified. That's because we can clearly see the private sector alone cannot solely respond and mitigate the risks of a hurricane. Both public and private sector resources working together help us survive a natural disaster when it "attacks" us.

By contrast, devastating cyberattacks are often "invisible." Without a powerful visual, it's easier to think of cyberattacks as an IT problem for the private sector to handle alone. In many cases, some level of public-private sector cooperation already exists. After the Capital One data breach, the company worked with the FBI to arrest the perpetrator and limit the damage. But in cases such as the Equifax data breach, some legislators, advocacy groups, media outlets, and members of the public took a purely punitive attitude that broadcasts the message that companies are on their own when protecting themselves from cyberattacks—and will be punished if they fail.

How does this narrative change if we think about cybersecurity from a national security perspective? For example, during World War II, German U-boats sunk hundreds of US ships. Why? We were not prepared, and we lacked public-private sector coordination. Did we tell commercial ships, businesses, and households that they were on their own? Did we punish them if they did not protect themselves at sea or turn off their lights? No. Eventually, the US learned that convoys (a public-private sector partnership) and blackouts (which must be implemented at the business and individual level) would together help fight against the U-boats. Once implemented, these tactics lessened the German attacks and the U-boats moved on to other targets.

Today, our approach to cybersecurity is slowly transitioning from our initial U-boat unpreparedness and heading toward a cyber equivalent of convoys and blackouts. However, we still have a long way to go until we reach the level of coordination the US shows when it handles a natural disaster like a hurricane.

This whitepaper will discuss why cybersecurity policy is not just a technology executive or cybersecurity industry problem. Everyone—lawmakers, non-technical business stakeholders, and the public—needs to care about cybersecurity policy and how our efforts to strengthen the public-private partnership positively affect national security. More specifically, this whitepaper will explain:

- Our current traditional (and wrong) mindset about where cybersecurity responsibility rests.
- What we must understand about the cyber enemy.
- The shared objectives of private sector CISOs, CEOs and boards, and the public sector.
- The ingredients of a strong public-private partnership.

Our Outdated Cybersecurity Mindsets Are Hurting Us

Many cybersecurity attacks, threats, breaches, incidents, and activities are unprecedented and take us into new territory. While some traditional, historical ways of thinking can help us make sense of cybersecurity, outdated mindsets can hurt us. When rules change, we need to throw the old rulebooks out.

Three mindsets in particular create significant obstacles to a public-private cybersecurity partnership:

- **All data breaches happen because a company is negligent**: Whenever a major data breach occurs, some lawmakers quickly hold hearings that ride the crest of temporary public outrage until the headlines die away. The company receives public humiliation for a few weeks, and then business as usual continues as the status quo returns. We react to every major data breach in such a similar way that it's like we follow a script—outrage, threats of punishment, Congressional testimony, headlines that eventually die off, and forgetting the whole thing in a matter of weeks until the next data breach. Continually reinforcing this "company is negligent" mentality means we teach the public to view cybersecurity as a failure of companies instead of a holistic issue related to international cybercrime (with companies as victims) and national security (with companies asymmetrically attacked by nation states).
- **All regulations are bad**: The NTSC is non-partisan, so we look at regulations on a case-by-case basis. With CISOs comprising our board, we understand the antipathy toward burdensome regulations. But even the most conservative CISOs point out the frustration of 54 data breach notification requirements strewn across 50 states and four territories, the fear of state data privacy laws headed in the same direction, and excessive compliance burdens from other redundant and contradictory cyber regulations. Pragmatic, reasonable standards are needed at a federal level so that CISOs can focus on protecting their companies. When regulations can reduce, streamline, and clarify compliance, then they are needed.

- **The military is our sole cyberspace defender against nation states**: Traditionally, the US military and intelligence communities have been our primary defenders against nation state adversaries. Cyberattacks blur this boundary between a traditional military attack and “silent” incursions by nation states in cyberspace. Nation states probe for vulnerabilities in critical infrastructure, steal intellectual property (IP) and personally identifiable information (PII), and implant ransomware such as WannaCry. Is WannaCry an attack on the US by North Korea, a criminal act attributed to cybercriminals, or just a business disruption? As cyberattacks began to threaten the public and private sector over the past few decades, the US found itself caught off guard similar to the German U-boats that used an entirely new method of attack. Our military and intelligence communities fought off cyberattacks in limited ways but operated under a “doctrine of restraint” until very recently. Today, US Cyber Command more proactively responds to cyberattacks but they need private sector partnership to fulfill their mission, especially because the majority of US critical infrastructure is owned by the private sector.

These three outdated mindsets ignore the nature of modern cyber adversaries. To change our mindset, we must understand the enemy we face.

The (Nearly) Invisible Cyber Enemy

Traditional military enemies operate in physical reality. When cyberattackers lack a physical presence, confusion can ensue when applying traditional military strategies to combat them. At the same time, we don't want to throw up our hands and leave all defense to the private sector. Cyber adversaries present the following challenges that disrupt our traditional strategies and tactics.

1. **(Nearly) invisible**: While we can sometimes pinpoint the origin of a cyberattack with a high level of certainty, adversaries often obfuscate their origin, location, and footprint to escape easy detection. For example, US and UK intelligence agencies recently discovered that an Iranian hacking group had actually been hacked by a Russian hacking group that used the Iranian hacking group as a cover for its own operation. Many other stories exist of cyberattackers disguised as other nation states or using cybercrime rings as fronts for nation state operations, leading to confusion about how to attribute cyberattacks to the correct adversary and respond appropriately. Obfuscation blurs the boundaries between nation states, cybercrime rings, and sophisticated criminals. And even if we identify the correct adversary, they will often never be punished or convicted because of nation states that protect the cyberattackers. Meanwhile, the barrier of entry to commit a cyberattack continues to decrease. For example, a cyberattack can be conducted by buying an Amazon Web Services (AWS) server with a stolen credit card number—leaving no immediate way to identify the attacker.
2. **Adversaries often move fast and only need one "win"**: The nature of cyberattacks is often asymmetrical. Strategies and tools such as endpoint detection and response (EDR)—defined by Gartner as "the tools primarily focused on detecting and investigating suspicious activities (and traces of such) other problems on hosts/endpoints"—have helped the public and private sector become more resilient against cyberattacks. However, the constant barrage of endless consequence-free trial and error attacks from nation states, cybercrime rings, and individual hackers means that while organizations can succeed in defending themselves 99.9 percent of the time, it's the 0.1 percent of the time they err that makes the papers, outrages the public, and leads to lawmakers excoriating companies. Also, new technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) threaten to keep cyberattackers at an asymmetrical advantage as they outpace current public and private sector security efforts.

3. **Adversaries going beyond breaches and data theft toward stealing ideas and threatening data integrity:** Cyberattacks have evolved from people simply trying to steal something (like accessing and emptying a bank account) and now involve trying to create new realities based on manipulating the integrity of data. Imagine if someone went into public records and changed the history of a deed of trust or a voting record. If we cannot trust that data is true or accurate, then our economy and national security is threatened. Threat actors also seek intellectual property, health records, new inventions, and other idea-based data that can hurt companies and the US economy in the long term. Currently, reputational damage and intellectual property theft are not covered by cyber insurance and remain uncharted territory for many companies.

To combat these adversaries, the public and private sectors cannot remain isolated from each other. It's helpful to examine the shared objectives of the public and private sectors to understand their common cause.

Shared Public-Private Sector Cyber Objectives

The US has great need for a comprehensive approach toward protecting our cyberspace—and the only way we're going to achieve this comprehensive approach is through a partnership between the public and private sector. Such a partnership helps strengthen national security, the US economy, and cybersecurity standards that help protect the government, businesses, and individuals. To strengthen this partnership, it helps to examine shared objectives, see how they align, and look at overall strengths and weaknesses.

	CISOs	CEOs and Boards	Lawmakers
Cyber defense and resiliency	Core priority to defend networks and make them resilient to attacks.	Companies need to be secure or they will go out of business.	Government systems need security to function.
Protecting customer/citizen data	Customer data (such as accounts) needs protection.	Protecting customer data affects brand trust and reputation while also establishing competitive advantage.	US citizen and resident data needs protection.
Data privacy	Data privacy compliance around authorized access to data (such as PII) is very important.	Complying with data privacy laws and protecting the privacy of data affects brand trust and reputation.	The strength of US data privacy affects our international reputation and must align with international standards. Our posture affects trade deals, international business, etc.
National security	Many CISOs use Information Sharing and Analysis Centers (ISACs) and partner with industry groups that share information with the public sector. Gives CISOs awareness of wider national security issues. While information sharing has improved, it still remains an issue for CISOs.	Not a priority for many, which is why organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) are conducting outreach directly to CEOs and boards.	National security is of highest importance, and cybersecurity is a subset of national security priorities. Too much focus on solely protecting government networks. CISOs often not at the table when laws and regulations crafted. Government promoting cyber threat intelligence sharing but still struggling with process, clearance, context, and relevance issues.

Let’s look closer at each shared objective:

- **Cyber defense and resiliency:** The public and private sectors both prioritize defending networks, but they often focus on protecting their own networks without considering their interdependency. If viewed from a broader perspective, cyberattacks can have a devastating impact not just on a single company but on an industry, the US economy, and critical infrastructure. Despite the best cyber defense, companies often cannot fend off a nation state alone. For example, the lesser of the two Yahoo breaches of 500 million users in December 2014 resulted from a cyberattack spearheaded by Russia’s Federal Security Service. Recent major data breaches are tied to attacks from Russia, China, Iran, and North Korea. The idea of cyber resiliency assumes constant cyberattacks will always take place and focuses instead on strategies that lessen the impact of cyberattacks, improve methods of countering cyberattacks, and strengthen networks so that it becomes incredibly difficult for cyberattackers to succeed.
- **Protecting customer and citizen data:** Without trust, business and government becomes much harder to run. Many small and medium-sized businesses go out of business after a data breach, and larger companies lose revenue, see their stock prices drop, and experience lost consumer confidence in their brand. With government, data breaches have affected the US voter database, veterans, government employees, and many other groups of citizens at the federal, state, and local level. Taken collectively, data breaches undermine our economy, trust in government, and national security.

- **Data privacy:** Protecting the privacy of data is different than preventing unauthorized breaches of customer or citizen data. Data privacy focuses on the legal and proper authorized access to data. Until recently, the US did not have much interest in strict data privacy requirements, which vary by industry. However, recent developments have made data privacy rise in priority across the public and private sectors because of:
  - Frequent compromises of intellectual property and PII.
  - The Facebook–Cambridge Analytica data scandal, which brought to light the extent of some corporate data collection efforts as well as how little consumer visibility exists pertaining to where data is shared or sold. According to the Pew Research Center in November 2019, today "a majority of Americans believe their online and offline activities are being tracked and monitored by companies and the government with some regularity."
  - The EU's General Data Protection Regulation (GDPR), which came into effect in May 2018, became the most prominent example of the global rise of regulatory frameworks focused on data privacy and protection.
  - The California Consumer Privacy Act (CCPA), which took effect in January 2020, sets strict data privacy standards that may precipitate other similar state laws. According to privacy expert Jodi Daniels, "Unlike GDPR, CCPA contains minimum thresholds businesses need to meet for the law to apply. […] Companies can be assessed civil penalties of up to $2,500 per violation, or up to $7,500 for intentional violations."
- **National security**: The idea of "collective defense" (with its cybersecurity connotation coined by Jeanette Manfra, formerly of CISA) means that cyber threat intelligence sharing between the public and private sector helps defend our nation. If only one company, sector, or industry holds onto or receives information without sharing, then that information may help one party but not everyone. As CISA Director Christopher Krebs pointed out back in 2017, a threat like WannaCry is better mitigated when everyone shares information with each other. As he said in a CNN opinion article in 2017, "We must ensure that indicators and information about cyber threats are shared broadly across the community so that more organizations can be inoculated against those threats. All entities—particularly those regularly targeted—benefit when the rest of the population can defend itself."

Currently, the shared objectives of CISOs, CEOs and boards, and lawmakers all align, but many of these shared objectives are carried out in siloed ways or seen as unimportant. Instead of struggling to achieve these shared objectives alone, strong public-private partnerships will allow us to achieve these shared objectives together.

The Four Ingredients of a Stronger Public-Private Partnership

The NTSC has taken actions to strengthen the public-private partnership by bringing together public and private sector stakeholders during events, meeting with government stakeholders (such as leadership at CISA) to encourage more partnering with the private sector, and meeting with members of Congress to promote the creation of legislation that assists with the public-private partnership—such as the Cybersecurity Advisory Committee Authorization Act of 2019 (H.R. 1975), which the NTSC vigorously supported in 2019.

From our efforts and collected input, we offer a few key strategies that will help continue to strengthen the public-private partnership.

1. Continue to form and support public-private sector collectives and advisory councils.

Forming and supporting collectives and advisory councils that work to bring the public and private sector together are essential, especially those that share cyber threat intelligence and ideas focused on "collective defense." Examples include:

- **ISACs**: Information Sharing and Analysis Centers (ISACs) exist for almost every industry and sector and share cyber threat intelligence with government. Some of the more mature ISACs such as the Financial Services ISAC (FS-ISAC) have existed since the late 1990s and serve as great models. By sharing intelligence and publishing alerts, indicators, and analyses to members, ISACs provide important input and feedback between the private and public sectors. As a collective group, they share information about viable threats so that organizations can prevent, target, and proactively squash these threats before they cause damage.
- **DHS (AIS)**: The Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS) program serves as a centralized capability for bidirectional cyber threat intelligence sharing. Historically, problems with AIS's information relevance and context combined with private sector apathy and wariness have worked to slow adoption. Sharing threat indicators in real time gleaned from DHS research and its partners, AIS has more than 250 entities (companies, ISACs, government entities) participating and distributes its intelligence to even more organizations through the partners of its participants. However, more participation is needed.
- **CISA**: In 2018, the Cybersecurity and Infrastructure Security Agency Act redesignated the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) as the Cybersecurity and Infrastructure Security Agency (CISA). Since then, CISA has made continual outreach efforts to the private sector, developed task forces such as the Cross Sector Information and Communications Technology Supply Chain Risk Management Task Force, and developed National Critical Functions defined as "functions of government

and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." CISA's efforts are helping bridge the gap between the public and private sectors.

- **Public-private sector advisory councils**: This idea is accelerating across many different aspects of government. Examples include:
  - **H.R. 1975**: The Cybersecurity Advisory Committee Authorization Act of 2019 will establish a panel of 35 highly proficient cybersecurity professionals to serve as subject matter experts to the Director of CISA and the Secretary of the Department of Homeland Security. The House Committee on Homeland Security advanced this bill in September 2018, its ideas (and the NTSC) were referenced in the long-awaited U.S. Cyberspace Solarium Commission's report to Congress, and the NTSC has worked with lawmakers and publicly supported the establishment of this advisory committee.
  - **State advisory councils**: Various state councils, task forces, and teams have formed since 2013 that combine expertise from the public sector, private sector, law enforcement, and academia. So far, 24 states have created these advisory councils.
  - **Local government advisory councils**: The ransomware attack on the City of Atlanta in 2018 stunned its leaders and forced a reevaluation of the way they thought about their information technology and cybersecurity—representing the same fate of many large and small cities across the United States. One post-ransomware attack strategy Atlanta implemented was a CIO Advisory Board comprised of both public and private sector CIOs and technology leaders. This trend could lead to more cities using such councils to create more dialogue and idea sharing between the public and private sectors.

While this existing activity seems plentiful, many of these efforts (with the exception of ISACs) are still in nascent or evolving form. And many of the best ideas about collectives and advisory councils are yet to come. While collaboration between the public and private sectors is headed in the right direction, efforts like H.R. 1975 and the underwhelming participation in AIS show that huge opportunities exist for more partnership. We need to take both existing and emerging collective efforts and focus on overcoming the obstacles and challenges that prevent public-private cyber threat intelligence sharing and partnering.

2. Strengthen proactive cyber defense and create a national agenda supporting effective cybersecurity policies.

As of a few years ago, the US government was not fully equipped as a nation to effectively fend off cyberattacks. We appeared as an open target much like the Germans saw the US as they attacked with their U-boats. One strategic approach to cyberspace that hurt both the public and private sector was our “doctrine of restraint” policy. Based on Department of Defense guidance in 2015, our government only responded militarily in cyberspace if attacked. Otherwise, our cyber deterrence strategy was passive and reactive. In the meantime, adversaries like Russia, China, Iran, and North Korea targeted critical infrastructure, interfered in our elections, stole intellectual property, and unleashed powerful ransomware—with few repercussions.

While our cyber deterrence is not anywhere near as established or sophisticated as traditional forms of deterrence, recent federal government efforts have built up more offensive capabilities. In the past few years, US Cyber Command has created greater capacity and added thousands of people to help fight adversaries in cyberspace. We are shifting from a “doctrine of restraint” to the equivalent of fighter squadrons warding off the enemy. As an example, this shift in strategy had a positive impact on protecting US elections from Russia in 2018 compared to 2016.

With efforts from entities such as US Cyber Command and CISA, the government has taken a more proactive approach to cyber defense. Yet, the majority of the nation’s critical infrastructure is owned by the private sector—which is why CISA and US Cyber Command focus on protecting it more as part of their evolving missions. But to protect critical infrastructure requires a strong public-private partnership and not just the solo efforts of the US government.

Part of strengthening proactive cyber defense also means creating an active national cybersecurity policy agenda that leads to policies that enable a public-private partnership to work. Otherwise, without the right policies we can’t have a real exchange of data and information sharing that supports cyber defense and resiliency, protects customer and citizen data, establishes data privacy, and protects national security. The NTSC’s policy agenda supports several important objectives across government and the private sector that are critical to the success of defending our nation such as:

- A national data breach notification standard
- A federal privacy standard
- Cybersecurity workforce development
- Protecting critical infrastructure
- Strengthening the public-private partnership

3. Rationalize and harmonize regulations, and work toward a national standard.

In April 2019, Jamie Dimon, CEO of JPMorgan Chase, noted that his company spends "almost $600 million on cyberdefenses." That's a lot of money, and all companies must spend a lot of money to secure their data and information. So why do we make it harder for them by passing or upholding impractical laws and regulations?

One of the biggest challenges for CISOs and companies is the lack of a national standard for important areas such as data breach notification and data privacy. Currently, our nation's companies—both US-based and multinationals—manage 54 different data breach notification rules and regulations across 50 states and four territories because Congress has been unable to pass a national standard despite repeated attempts. At quite a few NTSC conferences and events, many CISOs say they would comply with the strictest state data breach notification law as a national standard—as long as there is just one place to file. The current model of redundant notifications and varying standards across the country is not cost effective for companies or fair to consumers.

On the horizon, data privacy could go the same route. The strict CCPA seems to be inspiring other states to pass similar laws. If Congress does not pass a federal standard soon, data privacy could become just as tough for CISOs to implement as data breach notification. Impractical laws and regulations such as these are just two examples of how Congress can place burdens—both direct and indirect—on companies. In some cases (such as what many fear with the CCPA), laws and regulations may even prohibit companies from complying because they are too impractical and written without industry guidance.

We need better rationalization and harmonization of our regulatory environment that allows for effective cybersecurity risk management on the private sector side. At the same time, these laws and regulations need to help strengthen partnerships with the public sector while providing reasonable private sector enforcement.

4. Educate the consumer and citizen.

Often forgotten in the midst of laws, regulations, and companies is the role of the individual consumer and citizen. It's easy to think hopeless thoughts about getting the US population to become more cybersecurity-savvy. However, it's critical to educate people about the basics of network security and security vulnerabilities—and it's possible.

First, if children are taught cyber hygiene essentials, we will not only begin to solve a long-term problem of cyber educating our citizens (similar to how kids learn about fire prevention in ways that carry into their adult years) but they will also transmit those messages to their parents. For example, many recycling campaigns originated with schoolchildren taking home key messages that explained the benefits to parents. Second, adults are most susceptible to training at work where they spend most of their time and have the most incentive to adopt new habits. However, many employers don't provide cybersecurity training, provide it as a one-off onboarding item, or provide it periodically (such as quarterly or monthly). According to research from Mimecast, "About half of those surveyed said their employer doesn't provide mandatory cybersecurity training. About 10% provide the training as optional for employees. Roughly the same number of employees said they only received formal cybersecurity training during the onboarding process when they began their employment."

Instead, we may consider the Japanese concept of "kaizen." The word means "continuous improvement" in the context of business, specifically connoting the idea that everyone in a company—from the CEO to entry-level employees—has a responsibility for the betterment of the company. Famously with Toyota, any employee could stop an assembly line to point out a defect—and they were rewarded for it, even if it meant productivity temporarily stopped or slowed. Thinking of kaizen, how can we reward—rather than punish or ignore—employees who practice security oversight?

Today, many companies have started to reward employees who take actions that reflect a knowledge of cyber hygiene fundamentals. PwC used gamification (by way of a *Game of Thrones*-inspired cyber simulation called "Game of Threats") to teach cybersecurity skills to senior executives. Companies conducting phishing email exercises often reward employees who detect the scam instead of just focusing on those who fall for it. If employees attend security training or show a willingness to follow best practices, some companies give them awards such as money, gift cards, or free meals. For example, employees who use two-factor authentication (2FA) may receive some kind of bonus or incentive.

Sadly, despite many companies beginning to reward employees, we still face an uphill psychological battle. For decades, business and government has marketed convenience to consumers—and this convenience has extended to technology. Consumers just want to plug in something and see it work. Compounding the problem, security is often anything but convenient. As we all know, securing one's computer, tablet, or smartphone and continually upgrading the operating software and apps is messy and hard, and consumers often don't really understand these processes. That's why so many computers and smartphones go unpatched and do not get updated. People also trust large brands and assume their bank is securing their account or Apple is taking care of security on a person's iPhone.

While some companies do a better job of helping consumers secure data and devices than others, it's still a person's responsibility to perform their end of the cybersecurity deal. A company cannot hold a person's hands to get them to patch software, update apps, and avoid clicking on malicious links and attachments. As a nation, we need cyber hygiene essentials communicated more regularly and frequently at the individual level to educate people about the seriousness of cyber threats. Similar to how a person's house lit at night could affect Germans attacking the US during World War II, people need to understand how their actions can affect national security. Describing a full list of cyber hygiene best practices is out of scope for this whitepaper but some basics include patching software and apps, running antivirus software, not clicking on suspicious links or emails, downloading software and apps from trusted sources, and backing up data.

Many companies do educate people at work, but the employee needs to start taking that discipline home. And companies need to create more of a culture of security that goes beyond periodic or one-off training, perhaps inspired by kaizen. If employees see something suspicious or witness an incident that threatens cybersecurity, then they need to know how to spot the risk and report it. Cybersecurity is not just the job of the CISO. It's a company-wide responsibility, and everyone has the responsibility to be secure.

Conclusion

If we look back across history, events that once seemed bleak where we battled against the odds ended up as some of our country's greatest learning moments. Not only did we learn but we also succeeded beyond our wildest dreams. Our government, businesses, and citizens worked together to frustrate Germany's U-boats and eventually drove them from our coasts. Our government, businesses, and citizens learned enough about hurricanes and other natural disasters to anticipate them and mitigate the risks as best as possible—lessening loss of life through proactive, coordinated evacuations and helping everyone rebuild their lives in the aftermath. In an extreme example, Russia's space dominance in 1957—which signified a national security threat as much as a scientific advance—spurred an unprecedented wave of public and private sector focus on science and technology that not only led us first to the Moon in 1969 but also planted many seeds for the US's science and technology dominance throughout the rest of the 20th century and into the 21st.

After some hard lessons, we are optimistic that our cybersecurity path will bear the same fruits—but we need to start our shift in mindset now. By changing our mindset, identifying the nature of this new adversary, understanding our shared objectives, and strengthening the public-private partnership, we can collectively defend the cybersecurity of our nation in a way that benefits government, business, and citizens. The NTSC supports policies and actions that help strengthen the public-private partnership—and we need the help of lawmakers, policymakers, and industry influencers to help us change our cybersecurity mindset across the public and private sectors as a way to strengthen our national security. Soon, we will respond to these invisible hurricanes with the same confidence and success as real ones.

NTSC
NATIONAL TECHNOLOGY
SECURITY COALITION

To learn more about the NTSC, visit us at ntsc.org.