Why We Need the Emerging Voice of the Chief Information Security Officer in Washington, D.C.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION
ntsc.org

A chief information security officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. While in the past the role was rather narrowly defined along those lines, nowadays the title is often used interchangeably with chief security officer (CSO) and VP of Security, which indicates a more expansive role in the organization. Moreover, CISOs increasingly report outside IT to their company's CEO, General Counsel, or Board of Directors. This is a significant shift over the past five years, reflecting how cybersecurity has become an issue of global importance to businesses as well as government. In the United States, increasingly severe cyber threats have established cybersecurity as not only a national security issue, but an economic issue that CISOs confront every day.

While CISOs have become more prominent within their own businesses, that prominence hasn't necessarily translated to public policy. At any given time, the government drafts and enacts a variety of cybersecurity legislation and regulations that will affect businesses. Traditionally, CISOs have not had much input into this process, even though they are the ones primarily responsible for the implementation of these cybersecurity laws and regulations.

Our vision is to help shape and influence national cybersecurity policy by becoming both a trusted partner and go-to resource for policymakers.

When lawmakers and regulators enact laws and regulations without CISO input, CISOs find that those requirements are overly burdensome or difficult to implement. In many cases, the objective of a law or regulation could have been achieved with language more aligned to the reality of cybersecurity, and that precise language, informed by CISOs, would have led to more secure companies.

Because of these concerns, the National Technology Security Coalition believes that CISOs need to become more involved in the public policy process. Our organization offers CISOs and other cybersecurity stakeholders a national platform to discuss important cybersecurity policy issues and generate insightful input to help positively influence public policy at its early draft stages. Currently, the NTSC actively advocates for specific policy priorities in Washington D.C., and CISO members regularly communicate with lawmakers and policymakers.

The NTSC is committed to ensuring the voice of the CISO is heard. Our vision is to help shape and influence national cybersecurity policy by becoming both a trusted partner and go-to resource for policymakers. Now in our sixth year, we've already made great progress toward that goal; many lawmakers and policymakers now reach out to us as they draft laws, regulations, and policy.

We see high demand for an organization like ours, suggesting the CISO's voice is both needed and welcome. With a broad membership of CISOs across many different industries and companies, we approach important cybersecurity policy issues with a non-partisan, industry-agnostic, holistic, and practical viewpoint.

In this whitepaper, we will look more closely at why the voice of the CISO matters in Washington, D.C.

Who Speaks for CISOs in Their Absence?

Just a short five years ago, most CISOs reported to the Chief Information Officer or Chief Financial Officer of an organization. Today, over 60 percent of CISOs report directly to an organization's Board of Directors or CEO. This percentage continues to grow daily, and it's easy to understand why.

Major cyber breaches have become frequent events. Just this year, headlines include Solar Winds, T-Mobile, The Florida Water System, Kroger, Microsoft Exchange, Colonial Pipeline, and LinkedIn. Ransomware. Data breaches. Nation-state hackers. Ongoing cyber risks to national security. Crippling costs to businesses from cyber-attacks. Personal information stolen or left unprotected.

Cybersecurity has become one of our most prominent national issues. It crosses all boundaries, affecting all companies, all industries, and all people. From our most critical infrastructure to mom-and-pop shops, cybersecurity touches everyone's lives.

However, when lawmakers and policymakers create cybersecurity legislation and regulations to address these serious issues, whose voice do they hear in the CISO's absence?

Industry groups: Financial services, retail, healthcare, and other industry groups often talk about cybersecurity issues and concerns with lawmakers through the lens of their own industry. For example, financial services and retail have incredibly different points of view about national data breach notification legislation and may provide lawmakers with contradictory information.

Privacy advocates: Many advocacy groups focus on consumer privacy and have a prominent voice in Washington, D.C. While many of these groups have excellent intentions, they often lack business pragmatism and recommend punitive rather than practical solutions.

Influential businesses: Major multi-billion-dollar organizations are regularly tapped to talk to lawmakers. These CEOs only represent those individual businesses, though, and only sometimes speak on behalf of an industry. They do not serve as a collective voice on cybersecurity.

Silicon Valley tech companies: On the surface, it might seem like these companies would provide the perfect leaders with whom lawmakers can discuss cybersecurity. But these influential vendors often look at cybersecurity from a vendor's perspective. They are developing and selling products and services related to cybersecurity, and self-interest can creep into conversations about cybersecurity legislation and regulations.

Certainly, these groups have a role to play in the national dialogue about cybersecurity legislation. The problem arises when lawmakers and policymakers only hear from these groups. When that happens, their views on cybersecurity become extremely limited. Because lawmakers do not live and breathe technology every day as part of their jobs, they often struggle to receive objective viewpoints about cybersecurity and learn for certain whether certain laws or regulations positively or negatively impact businesses and consumers.

The reality is that cybersecurity spans not only all industries, but all of government as well. What impacts one company or industry can impact all companies, organizations, and government entities. If lawmakers do not hear from the security practitioners in the trenches, then a critical piece of the overall picture is missing when legislation, regulations, and policies are drafted.

Until recently, the CISO's voice has been relatively unheard on the Hill. But these C-level executives are exactly the voice that legislators need to hear.

What the CISO's Perspective Offers Lawmakers

CISOs can provide fresh, useful insights and ideas to help address the most serious security issues that face our country.

CISOs can provide fresh, useful insights and ideas to help address the most serious security issues that face our country. They represent a practical, practitioner, and often industry-agnostic point of view. They're the ones in the trenches of thousands of American businesses battling against the countless barrage of cyberattacks. They secure information ranging from intellectual property to personally identifiable information (PII), all while complying with many federal and state regulations that often hinder—rather than help—their efforts. CISOs are:

Practical: Many laws and regulations are aspirational or punitive, articulating an ideal of what should be rather than what is practical or useful. Like everyone else, CISOs want to protect consumers and avoid data breaches, but because of their daily experiences, they often see a more pragmatic path forward.

Practitioners: CISOs are defending companies every day in real time. They see cyberattacks occurring 24/7. They know what it takes to defend companies, how compliance helps or hinders their activities, and what help is needed from outside sources such as the federal government. Unlike industry groups, vendors, and privacy advocates, CISOs live cybersecurity every day.

Industry-agnostic: While it is true that CISOs may join groups of industry CISOs in united efforts, CISOs by nature tend to be industry-agnostic. They see cybersecurity from a higher-level perspective and understand how threats impact all businesses. They recognize that ultimately there must be a whole-of-nation approach to cybersecurity, which requires looking through a larger lens than just their industry or enterprise.

The unintended consequences of cybersecurity legislation often hinder a CISO's main job: securing their organization. Some examples of the repercussions from failing to involve the practical, practitioner, and industry agnostic CISO's point of view are detailed below.

Data Breach Notification

Despite bipartisan support, we still do not have a national data breach notification law. Instead, after a data breach, CISOs must individually report to 50 states, the Virgin Islands, Guam, Puerto Rico, and the District of Columbia. Consumers are not protected equally in all states, and it's reasonable to question why so many different and varied laws exist, especially when many seem to focus more on satisfying regulators rather than following a nationally agreed upon set of data breach notification standards.

Without hearing from CISOs, we find that lawmakers still do not understand how much of a CISO's team is devoted to compliance with the day-to-day burdens of so many different federal, state, and territorial data breach notification laws. Ironically, in this case, "states' rights" actually leads to overregulation.

Cyber Threat Intelligence Sharing

Major issues still exist with sharing threat intelligence information through public and private sector exchanges that create value for both sectors. A glaring example of this problem occurred with the 2017 WannaCry ransomware attack the root cause of which was that the NSA held on to a cybersecurity vulnerability. This situation illustrates concerns about the Vulnerabilities Equities Process, a process in which the federal government decides whether to disclose or utilize software security vulnerabilities, and information sharing between federal agencies and companies.

As CISOs try to defend themselves from cyberattacks, they often lack the best information necessary to anticipate attacks, understand their attackers, and deploy the correct response. While public-private cyber threat intelligence exchange is improving, it's still not ideal. CISOs want to know whom to address at the federal level, receive information in a direct, consistent way, and learn more from the US government about adversaries. Even the most pro-business CISOs admit they need some help from the US government concerning intelligence, defense, and legal responses to the sophisticated cyberattacks that they cannot fight off by themselves.

Data Privacy

National privacy legislation is on lawmakers' radar because of the likelihood that, if they do nothing, states will make their own laws. The California Consumer Privacy Act (CCPA) has served as a launching point for many ongoing discussions about national privacy laws. Much of the discussion is centered around definitions (e.g., "personal information") and specifics (such as the practicality of a 72-hour response time to a data privacy incident).

> **The most effective and meaningful approach toward solving data privacy problems is a single comprehensive bill.**

This would preclude a flurry of state laws such as the California Consumer Protection Act (CCPA), the Colorado Privacy Act, and Virginia's Consumer Data Protection Act (CDPA). Such a bill should address components of defining data, protecting data, establishing minimum standards of care, and outlining uniform notification rules. Unitary requirements would ensure that citizens have equal protection wherever they reside or wherever their data is stored. For example, the International Association of Privacy Professionals (IAPP) notes nine different consumer rights and eight different business obligations commonly seen across many state laws. Such principles would serve as an excellent starting point for discussions about what a federal privacy law should require for consumers and businesses.

The NTSC Helps CISOs Quickly Impact Washington D.C.

Since its launch in 2016, the National Technology Security Coalition has received significant validation for its mission to amplify the voice of the CISO in Washington, D.C. We are a non-profit, non-partisan organization that serves as the preeminent advocacy voice for CISOs. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

> We unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

That's our mission statement, and we've consistently validated it with action since we began six years ago. It's clear the NTSC is already having an impact on the Hill.

A few examples include:

Immediate Bipartisan Interest and Support:

Early supporters of the NTSC included Representative John Katko, the ranking member of the House Homeland Security Committee, Representatives Michael McCaul (R-TX), Chairman Emeritus of the House Homeland Security Committee and co-chair of the House Congressional Cybersecurity Caucus, and Jim Langevin (D-RI), co-chair of the House Congressional Cybersecurity Caucus.

Ongoing Dialogue and Involvement with DHS: To combat the perception of a chasm between the public and private sector, the NTSC has established a healthy, honest dialogue and increased involvement between CISOs and the Cybersecurity and Infrastructure Security Agency (CISA), the cyber arm of DHS. This has included CISA participation at NTSC events and conferences, meetings on the Hill, public support for the National Risk Management Center, and publishing a whitepaper outlining CISA's role in our collective defense as it relates to the private sector.

Introduction of the Cybersecurity Advisory Committee Authorization Act:

The NTSC supported and advocated for bipartisan legislation introduced by Representative John Katko (R-NY) in the House of Representatives and Senators David Perdue (R-GA) and Kyrsten Sinema (D-AZ) in the Senate to establish the Cybersecurity Advisory Committee (CSAC). With bipartisan support, the Cybersecurity Advisory Committee Authorization Act, which was included in the National Defense Authorization Act of 2021, established an advisory committee of 35 cybersecurity professionals from across industries. The committee will provide the Director of CISA and the Secretary of DHS guidance on cybersecurity policy and rulemaking. According to Rep. Katko, "By creating a Cybersecurity Advisory Committee, we can facilitate a vital dialogue between public and private partners and better secure the U.S. I'm grateful for the support of our private partners for this initiative, including the National Technology Security Coalition, and I look forward to working with them to expand public-private engagement in cybersecurity."

Support of CISA:

The NTSC is supportive of and in close dialogue with key stakeholders in CISA, including newly appointed Director Jen Easterly, who will serve as the opening keynote speaker at our 2021 National CISO Policy Conference in Washington, D.C. We applauded the passage of the Cybersecurity and Infrastructure Security Agency Act by the US Senate in October 2018. This bill redesignated DHS's National Protection and Programs Directorate (NPPD) as CISA. The NTSC supported this legislation because it reflects the needs of the private sector to work more productively with DHS to share cyber threat intelligence and communicate about critical cybersecurity issues that affect national security. A dedicated agency with a clear mission, such as CISA, helps DHS carry out this important work.

Advantages of Working with a Non-Partisan, Industry-Agnostic Group of CISOs

Together, CISOs representing these companies present a powerful, insightful, and unified voice that lawmakers can rely on without vendor or industry bias.

The NTSC takes positions on issues related to national cybersecurity policy and communicates about those issues to lawmakers. We have presence and visibility on the Hill and regularly meet with lawmakers, regulators, and influencers. As a result, lawmakers and DHS are already familiar with the NTSC as a trusted resource after only a few years of existence.

The company names on the NTSC Board of Directors represent major national companies including Aaron's, Aflac, Arizona State University, BNP Paribus, Cardinal Health, Cisco Systems, Comcast, Discover Financial Services, Dollar Tree, Edward Jones Investments, Eli Lilly & Company, Eonia Consulting, Equifax, Globe Life, Graham Holdings, Hearst, Huntington Bank, ICE, Johnson & Johnson, JPMorgan Chase & Company, LabCorp, Mastercard, McKesson, Microsoft Corporation, Motorola Mobility, NCR, NeilsenIQ, Norfolk Southern Corporation, Oceaneering, RedSeal, Inc., Republic National Distributing Company, Sage Group, State Street, Synovus, TaxSlayer, Technology Association of Georgia, TransUnion, Unisys, US Bank, Voya Financial, and Western Digital. Together, CISOs representing these companies present a powerful, insightful, and unified voice that lawmakers can rely on without vendor or industry bias.

Finally, the voice of the CISO is being heard. Lawmakers and policymakers pick up the phone and reach out to us more frequently than before. In the long-term, we will continue our dialogue, education, and congressional outreach while growing our membership with CISOs and security practitioners around the country. As a conduit between the public and private sector, we are making sure that the dialogue and work we do in Washington, D.C. gets shared with our membership.

As a young but vital organization, we're just getting started. We look forward to speaking with you about national cybersecurity policy and assisting you in protecting our nation's security through a stronger partnership between the public and private sector that also benefits both businesses and consumers.

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan organization that serves as the preeminent advocacy voice for Chief Information Security Officers (CISOs) across the United States. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

4400 North Point Parkway
Suite 155
Alpharetta, GA 30022
ntsc.org