NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

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

By Patrick Gaul
Executive Director
National Technology Security Coalition

Chief Information Security Officers (CISOs) increasingly report outside IT to their company's CEO, General Counsel, or Board of Directors. This is a significant shift from even five years ago, reflecting how cybersecurity has become an issue of global importance to both businesses and government. In the United States, cyber threats of increasing severity make cybersecurity both a national security issue as well as an economic issue that CISOs confront every day.

While CISOs may 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 passes a variety of cybersecurity legislation and regulations that will affect businesses. Traditionally, CISOs have not had much input into this process—and yet they are the ones who primarily must implement cybersecurity laws and regulations.

When lawmakers, regulators, and public policymakers create laws and regulations without CISO input, CISOs find that requirements sometimes don't make sense or they're not doable. 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.

The National Technology Security Coalition believes that CISOs need to become more involved in the public policy process because of these issues. Our organization offers CISOs and other cybersecurity stakeholders a national platform to discuss important cybersecurity policy issues and generate insightful input that helps 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.

After a long silence, the NTSC is making the voice of the CISO heard. Our vision is to help shape and influence national cybersecurity policy, becoming both a trusted partner and go-to resource for policymakers. Now in our fourth year, we've already made great progress toward that goal as many lawmakers and policymakers have started to 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 covering 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—and that percentage increases every day.

It's easy to understand why. Just look at the headlines during the last two years. Capital One. Equifax. Facebook. Marriott. WannaCry. NotPetya. Ransomware. Data breaches. Nation-state hackers. Ongoing cyber risks to national security. Crippling costs to businesses from cyberattacks. People's personal information stolen or left unprotected.

Clearly, 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 particular industry. For example, financial services and retail have incredibly different points of view about national data breach notification legislation.
- **Privacy advocates**: Many lobbying 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 businesses are regularly tapped to talk to lawmakers, but these CEOs only represent those individual businesses—and only sometimes speak on behalf of an industry. They are not providing a collective voice about cybersecurity.
- **Silicon Valley tech companies:** On the surface, it might seem like these companies would provide the perfect leaders with whom to talk cybersecurity. But these influential vendors often look at cybersecurity from a vendor's perspective. They are selling products and services related to cybersecurity, and self-interest can creep into conversations about cybersecurity legislation and regulations.

Certainly, each of these groups has a role to play in the national dialogue about cybersecurity legislation. The problem is 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

know for certain whether certain laws or regulations positively or negatively impact businesses and consumers.

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

Until now, the CISO's voice has been relatively unheard on the Hill. But these C-level executives are exactly the voice that needs to be heard.

Why the CISO's Voice Provides a Missing Perspective

CISOs can provide fresh, needed insights and ideas to help address what's quite possibly the most serious security issue now facing 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 millions of cyberattacks, securing information ranging from intellectual property to PII, and complying with many federal and state regulations that often frustrate—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 actually should and can happen. Like everyone else, CISOs want to protect consumers and avoid data breaches, but they often see a more practical path forward based on their daily experiences.
- **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. It's their job.
- **Industry-agnostic**: Yes, CISOs may join groups of industry CISOs in united efforts. However, CISOs by nature tend to be industry-agnostic. They see cybersecurity from a higher-level perspective and understand how threats impact all businesses.

The unintended consequences of cybersecurity legislation often hinder a CISO's main job—securing their organization. Some examples of the repercussions from not involving the practical, practitioner, and industry-agnostic CISO point of view include:

Data Breach Notification

Despite bipartisan support, we still currently 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, so it's reasonable to challenge why so many different and varied laws exist that seem to focus more on pleasing regulators rather than following a nationally agreed upon set of data breach notification standards.

Without hearing from CISOs, we find that lawmakers would not necessarily realize the high percentage of a CISO's team devoted to compliance and the day-to-day burdens of so many different state and territorial data breach notification laws. In this case, states' rights actually lead 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. Its root cause? The NSA holding onto a cybersecurity vulnerability. This situation illustrates concerns about the Vulnerabilities Equities Process and information sharing between federal agencies and companies.

As CISOs try to defend themselves from cyberattacks, they often do not have the best information to anticipate attacks, understand their attackers, and fight back with the correct response. While public-private cyber threat intelligence exchange is improving, it's still not ideal. CISOs want to know who 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, defenses, and legal responses to sophisticated cyberattacks that they cannot fight off by themselves.

Data Privacy

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

An effective and meaningful approach toward solving data privacy problems is a single comprehensive bill—avoiding the flaws of GDPR or a flurry of state laws such as the CCPA—addressing 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 seen across many state laws. Such principles would serve as an excellent starting point for discussion about what a federal privacy law should require for consumers and businesses.

The NTSC Helps CISOs Quickly Impact Washington D.C.

Launched in 2016, the National Technology Security Coalition has received significant validation of 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.

That's our mission statement, and we've consistently validated and backed it up with action since our start just three years ago. It's clear the NTSC is quickly having an impact on the Hill.

A few examples include:

- **Immediate Bipartisan Interest and Support**: Early supporters of the NTSC included Michael McCaul (Chairman Emeritus on the House Homeland Security Committee) and Jim Langevin (founder and co-chair of the House Cybersecurity Caucus). The NTSC quickly became a go-to voice for the House Cybersecurity Caucus and we have been in continual dialogue with these lawmakers from the start.
- **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 (where DHS is receptive to criticism) and increased involvement between CISOs and DHS. This has included DHS participation at NTSC events and conferences, meetings on the Hill, public support for the National Risk Management Center and CISA, and publishing a whitepaper outlining DHS's role in our collective defense as it relates to the private sector.
- **Introduction of the Cybersecurity Advisory Committee Authorization Act of 2019**: The NTSC influenced and supported bipartisan legislation introduced by Representatives John Katko (R-NY), Dan Lipinski (D-IL), Dan Newhouse (R-WA), and Brian Fitzpatrick (R-PA) to establish the Cybersecurity Advisory Committee (CSAC). With 14 Democratic and eight Republican co-sponsors, the Cybersecurity Advisory Committee Authorization Act of 2019 will establish an advisory committee of 35 cybersecurity professionals from across industries to provide the Director of the Cybersecurity and Infrastructure Security Agency (CISA) and the Secretary of the Department of Homeland Security (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 has been supportive and in close dialogue with Christopher Krebs, Director of CISA. 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 such as the CISA, with a clear mission, helps DHS carry out this important work.

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

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, regularly meeting with lawmakers, regulators, policymakers, and influencers. As a result, lawmakers and DHS already know about 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, Dollar Tree, Ellie Mae, Freddie Mac, Globe Life, Hewlett Packard Enterprise Services, Huntington Bank, Johnson & Johnson, JPMorgan Chase, Mastercard, McKesson, Motorola Mobility, NCR, Oceaneering, Ohio State University, Synovus, TaxSlayer, Technology Association of Georgia, TransUnion, Unisys, United Airlines, US Bank, VF Corporation, Voya Financial, WarnerMedia, and Western Digital. Together, CISOs representing these companies present a powerful, insightful, 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 and more. In the long-term, we will continue our dialogue, education, and congressional outreach while increasing 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—and we look forward to talking to 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.

To learn more about the NTSC, visit us at ntsc.org or reach out to Patrick Gaul at patrick@ntsc.org or 404.920.0703.