STATE OF MAINE
DEPARTMENT OF
ADMINISTRATIVE AND
FINANCIAL SERVICES,
OFFICE OF INFORMATION
TECHNOLOGY

STRONGER TOGETHER: BUILDING RESILIENCE FOR A CYBERSECURE TOMORROW

NASCIO 2021
State IT Recognition Awards
Maine Cybersecurity Advisory Council – A Whole of Government Approach

Category:
Cybersecurity

Project Initiated:
June, 2019

Project Completed:
January, 2021

Nomination Submitted by:
Fred Brittain, Chief Information Officer
State of Maine
Fred.Brittain@maine.gov
207-4417631

EXECUTIVE SUMMARY

The State of Maine Executive Order creating the Maine Cybersecurity Advisory Council signifies the State's commitment to recognizing the importance of building partnerships across all levels of government to meet the threat posed by this new cyber threat ecosystem. The implementation of a much-needed governance framework demonstrates that Maine is leading the way for prioritizing the management of its cybersecurity risks, dedicated towards strengthening our ability to detect, respond and recover from cyber events.

The Office of Information Technology's (OIT) Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) worked closely with the Governor's Department of Administrative and Financial Services (DAFS) leadership team to lay the groundwork across the enterprise to develop a broader appreciation of the cyber threat landscape. This included identifying best practices for building the State's cyber resiliency, and for developing a collaborative approach to creating partnerships at the federal, state and local level. Building awareness of the risk and the need for change in this arena took significant lines of effort, as cybersecurity had previously been approached within silos and not as part of a whole of government approach.

This effort demonstrates the State's leadership in taking on its cybersecurity challenges as a team effort, committing to build stronger partnerships with government, law enforcement and state and local entities, all focused on strengthening our defenses, and ultimately increasing our cyber resilience. Moving forward, the State is poised to strengthen its role within the larger cyber ecosystem- facing the threat together as a team for the benefit of all Maine citizens.

PROJECT NARRATIVE

CONCEPT

After a year of what U.S. Department of Justice officials have described as the costliest year on record for crippling cyberattacks, Maine, like so many of other states, has been playing a catch-up game to ramp up its defenses against increasingly sophisticated cyber threats. This cyber threat ecosystem is dauntingly complex, and, as a small state, we have been stretching our capabilities and limited resources to the maximum extent possible. Over recent years, OIT has been sharpening its focus on advancing its cybersecurity posture to safeguard the State of Maine's information assets in response to the dramatic rise in cybersecurity threats. This cyber ecosystem has brought an unprecedented level of cyber threats to the door of state and local governments during a pandemic, and executive leadership recognized that threats posed a very real risk to the continuity of government and security of our citizens.

Just like its state partners across the country, Maine's response was hindered by outdated security paradigms ill-equipped to manage this new threat landscape. Fraught with challenges from decades old IT systems and limited resources, as well as a suddenly activated large remote workforce, the cyber threats were ramping up during the pandemic, adding to the complexity of State's pandemic response efforts. During these challenging times, State leadership made the difficult choice to tackle the cyber threat head on, knowing that hard work would need to be done to prioritize action at the State level to secure our network defenses against these very real and debilitating cyberattacks.

Without an effective governance structure, efforts were made in silos, lacking the structure to break down barriers in communication due to slow communication channels. Disparate levels of effort were being made across agencies to implement cybersecurity controls lacking a uniform approach the enterprise. Executive leadership recognized that these challenges were impacting the State's security, hindering our capability to identify and manage the complex onslaught of cyber risks and provide a coordinated, effective response.

Executive leadership took unprecedented steps to make cybersecurity governance an enterprise-wide priority. The CISO and CIO began holding regular briefings that involve senior management on IT security and policy governance and strategic planning matters. In addition, IT leadership established an Information Security Governance Working Group and IT Leadership Council to improve the information process flow among agency leaders, raise the awareness of the importance of IT security in all branches of government, as well as involve their perspectives within the broader strategic planning process. Enhanced governance initiatives began to take

shape, including an effort to modernize agency policies and procedures to align with NIST standards. This took time to develop broad buy-in on the importance of developing best practices for information security throughout all aspects of IT. By involving a broad spectrum of IT and agency leadership, the foundation was being developed for a broader understanding of risk at all levels of government.

The effort took roughly two years of preparations and development, which dovetailed with OIT's efforts to update its strategic plan. These efforts were essential to identify the best pathways for enhanced cyber communication within the State and would serve as a vehicle for broad change and support for modernizing the State's cybersecurity defenses. OIT and DAFS leadership worked with the Executive Branch to build awareness of the need for a new Council that would remove barriers in communication channels and build relationships among key stakeholders across the State. Support and advocacy among these stakeholders ultimately culminated in the signing by Governor Janet Mills of the Executive Order establishing the State of Maine Cybersecurity Advisory Council (Council) https://www.maine.gov/governor/mills/sites/maine.gov.governor.mills/files/inline-files/EO%2082%2025.pdf

The Governor's Executive Order the Council represents a significant step forward for Maine's cybersecurity governance framework. The Council will align and prioritize cybersecurity activities with our State's overall risk tolerances and resources. The Council will serve the following goals:

- Lead a statewide, collaborative effort across a wide array of stakeholders to enhance Maine's cybersecurity;
- Develop a cybersecurity framework and governance structure that is aligned with national best practices, including those developed by the National Institute of Standards and Technology (NIST), across all levels of government to safeguard the data entrusted to the State;
- Strengthen our cross-agency coordination, information sharing, preparation and emergency response capabilities to protect the State's computer networks and critical infrastructure systems against a broad range of cybersecurity risks;
- Provide recommendations focused on narrowing the cybersecurity workforce gap and developing a talent pipeline in fields involving cybersecurity;
- Support collaborative efforts with the Homeland Security Advisory Council to identify cyber threats and align emergency and cyber response and recovery operations; and
- Establish an effective cybersecurity communication chain to the Governor's Office.

SIGNIFICANCE

The significance of the Council's work is illustrated by its prioritization of several lines of effort that reflect concerns universal to all states. First and foremost, it prioritizes the implementation of a cybersecurity and governance framework aligned with the NIST, essential to advancing the State's efforts to strengthen its security requirements to safeguard information assets and meet a complex array of federal mandates governing the protection of federally-protected data entrusted to the State. The Council's work will also be impacting *two* of the **NASCIO State CIO Top Ten Priorities for 2021**, including #1: Cybersecurity and Risk Management and #5: Budget, Cost Control, Fiscal Management. By addressing these two top concerns, the State will be having a greater discussion of its risk tolerance level across the enterprise, and as a result, will be able to make informed decisions on how to prioritize cybersecurity expenditures to mitigate the risks in a manner that will be in the best interest of the State.

Leadership and effective governance are critical components of a successful cybersecurity framework for the State of Maine. The Council serves as a much-needed vehicle to align our efforts with best practices, maximize the use of limited state resources, strengthen our partnerships at the federal and state level, and break down barriers in communication across agencies and branches of government to make the State of Maine more secure.

"I am excited to help lead this new Council as we endeavor to highlight areas of improvement, form stronger partnerships, and ultimately strengthen our collective security posture with the state against cyber threats. I thank Governor Janet Mills, Commissioner Kirsten Figueroa, and CIO Fred Brittain for their leadership, and recognizing the importance of proper cybersecurity."

Nathan Willigar, Chief Information Security Officer

In addition, the Council represents a significant step forward for the State in its cybersecurity maturity, focusing on breaking out of old silos to advance the State's cybersecurity readiness. This work will strengthen relationships and remove barriers in communication channels and enhance and develop key partnerships – all with the goal of safeguarding the State's sensitive data and information systems that serve the citizens of Maine. Efforts are underway to enhance the cybersecurity awareness of employees, as well as working with the State Legislature to move statutory language forward that ensures compliance with federal directives for the protection of sensitive data.

By engaging State and Federal partners on cybersecurity best practices, the State will manage limited resources more effectively and develop stronger defenses to secure the State's economy, critical infrastructure, and citizen's privacy. These efforts recognize that inaction exposes us to not only financial losses, but also the loss of the public's confidence in our institutions entrusted to safeguard their confidential and sensitive data. Raising awareness of the threats we face unifies us with the knowledge that we all have a critical role to play in reducing the risk of future cyber-attacks.

IMPACT

The Council will be a valuable tool in the State's cyber toolbox – from strengthening cyber awareness and incident response capabilities among federal, state and local partners to advancing a cybersecurity framework that aligns with NIST – the Council will advance a whole-of-state approach to reducing its cybersecurity-related risks; an approach that has already made inroads in strengthening the State's security policies and procedures. Moving forward, this approach will support and drive collaboration among state and federal agencies, local governments, the National Guard, healthcare and other critical sectors of the economy. By approaching cybersecurity as a team sport, the Council will be equipped to facilitate the sharing of time-sensitive information rapidly when an incident occurs and when timing is critical to reduce our exposure to attack, ensuring a more robust incident response.

Prior to the Council, the State lacked the structure and pathway to streamline cybersecurity communications across the enterprise. Moving forward, the Council will provide the structure for strengthening our collective understanding of risk across the State and broaden the discussion for how to best reduce our risks and make key investments that will shore up the State's defenses. A few years ago, prior to the work on the project, cybersecurity was "nice to have" but not viewed as an essential element across the enterprise. Now, the process has raised collaboration and a dialogue that elevates the discussion of how the critical challenges we face in this modern cyber ecosystem and will continue to enhance our learning and engagement at all levels of state government.

The Council will dovetail its work with OIT's strategic plan for an enterprise wide security governance framework that will foster cross-cutting conversations across the enterprise on issues of information security. The Executive Order also requires regular reporting to the Legislative branch to keep the group accountable and focused on its tasks, and ensures frequent communication with the Governor's Office on issues of immediate cyber importance, reducing the risk that critical issues will be lost in communication channels.

Follow-through will be critical to ensure that the Council's operational plans support the State's strategic efforts to identify gaps in that are revealed through risk assessments and identify the resources necessary to accomplish both short and long-term Council goals. This endeavor, although challenging, is worthwhile. Larger scale regional and national ransomware attacks, as evidenced by the most recent Colonial Pipeline attack, have the capability to severely threaten the daily lives of all Mainers and impact essential services. The Council will play a key role in creating a State of Maine that is both resilient and secure for the benefit of all Maine citizens, ensuring continuity of the Maine way of life.