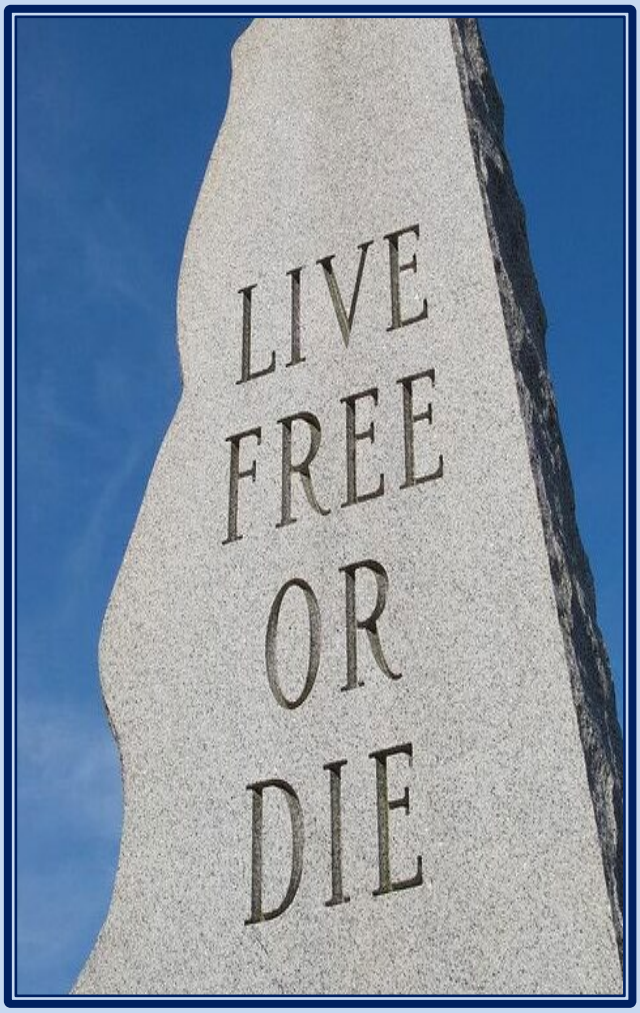


Building a Culture of Security in the Granite State's Human Intrusion Prevention Systems

The New Hampshire Municipal Cyber Defense Program

State: New Hampshire
Agency: Department of Information Technology
Category: Cross-Boundary Collaboration & Partnerships
Initiated: August 2022
Completed: August 2024

Ken Weeks
Chief Information Security Officer
kenneth.l.weeksiii@doit.nh.gov
(603) 931-9234

Executive Summary

New Hampshire has 10 Counties, 13 Cities, 221 Towns, 25 Unincorporated places, 139 K12 Public School Administrative Units (SAU), 223 Public Libraries and approximately 2,500 public water systems (Drinking water and Wastewater) across the State. Each of the 10 Counties has a Sheriff Department, Public Nursing Home, and Correctional Facility (Jail). Each of the 13 Cities and 221 Towns have a Police Department and Fire Department. Each of the SAUs have multiple schools (kindergarten, elementary, middle, and high schools) and some have multiple schools at the various levels. ***Granite Staters depend on each of these organizations to maintain and sustain our very way of life. Each of these New Hampshire Public Sector organizations is potentially under attack by malicious cyber actors from anywhere in the world, 24 hours a day, 7 days a week, 365 days a year!***

In August of 2022, three like-minded people sat down, broke bread, enjoyed a cigar and glass of bourbon (or two) and decided, "This is just unacceptable. We must figure out a way to accelerate increases in the cybersecurity readiness of the places we live, work, and raise our families – those [expletive deleted] don't get to win." Out of that discussion, The Senior Partner of the Atom Group, the Cybersecurity Risk Manager for the New Hampshire Public Risk Management Exchange (Primex^3) and the NH State Chief Information Security Officer (CISO) incubated the New Hampshire Municipal Cyber Defense Program (NH MCDP). The NH MCDP is a public-private partnership between The State of New Hampshire's Department of Information Technology (DoIT), NH PRIMEX and The Atom Group, who manages the program.

The NH MCDP team has grown well beyond "three like-minded people" and evolved into the primary vehicle for enhancing New Hampshire's Cybersecurity Readiness Services at the local level. This program is primarily funded by the NH Department of Information Technology through Homeland Security Grants and the State and Local Cybersecurity Grant Program (SLCGP) and the funding is available through 2027.

The MCDP is unique because the training and assessments are customized based on the organizations function, the trainees' roles and responsibilities, and the organization's existing cybersecurity readiness. It is universal because it applies to every NH Local Public Sector entity.

Since inception, the MCDP has provided service to 40% (4 of 10) of the counties, 46% (6 of 13) of the cities, 17% (37 of 221) of the towns, 40% (56 of 139) of the SAUs and 18% of NH First Responders. (In many cases engagements with Cities/Towns and their Police and Fire Departments are coordinated or integrated.) Planned and funded growth areas for the MCDP are NH Residents at Public Libraries (more than 10 have been provided), the SCADA Operators at NH Drinking Water and Wastewater systems
(more than 10 sessions have been provided.)

Through the NH MCDP, we are building a culture of security by increasing the knowledge of thousands of Human Intrusion Prevention Systems (HIPS) to NOT CLICK, making it more difficult for Malicious Cyber Actors to achieve their objectives against State and Local entities in New Hampshire.

Live Free or Die!

PART I: THE IDEA

The Problem: New Hampshire has 10 Counties, 13 Cities, 221 Towns, 25 Unincorporated places, 139 K12 Public School Administrative Units (SAU), 223 Public Libraries and approximately 2,500 public water systems (Drinking water and Wastewater) across the State. Each of the 10 Counties has a Sheriff Department, Public Nursing Home, and Correctional Facility (Jail). Each of the 13 Cities and 221 Towns have a Police Department and Fire Department. Each of the SAUs have multiple schools (kindergarten, elementary, middle, and high schools) and some have multiple schools at the various levels. Granite Staters depend on each of these organizations to maintain and sustain our very way of life. Each of these New Hampshire Public Sector organizations is potentially under attack by malicious cyber actors from anywhere in the world, 24 hours a day, 7 days a week, 365 days a year. In other words, Grifters are grifting, Phishers are phishing, and Clickers are clicking. New Hampshire systems are not being "hacked" into; they are being LOGGED into! ***So, how do we improve the capabilities of our Human Intrusion Prevention Systems (HIPS), otherwise known as "Users" and build a culture of security?***

Why Does it Matter?

- From January to the end of August in 2024, municipal entities in New Hampshire experienced 55 Cyber Incidents that were serious enough to result in a claim to the NH Public Risk Management Exchange (Primex^3).
- These attacks resulted in $472,878.37 of incident response expenses alone.
- The costs for complete remediation and recovery are conservatively estimated at $5-7M when aggregated across all 55 incidents.

Without exception, each incident was initially enabled by a failure of the Human Intrusion Prevention System (HIPS)!

Why is the NH MCDP Unique? The MCDP is different from the "Cybersecurity Awareness Training" all organizations complete. Awareness training is delivered via a weblink in an email. There is no "personal touch" and limited role-based training for users. Although necessary, this training is not sufficient!

The NH MCDP training and assessments are deployed in parallel with an organization's awareness training and Primex^3 ongoing cybersecurity training efforts, but also customized based on the organization's function, the trainees' roles and responsibilities, and the organization's existing cybersecurity readiness.

Cybersecurity training has been developed in response to data collected within the State of New Hampshire and addresses critical aspects of cybersecurity readiness. These training sessions are selectable by any municipality within the state and are delivered as 90-minute, 2-hour, 4-hour, and full-day trainings as workshops or through webinar format. Eleven of these programs were created and added between October 1, 2022, and December 15, 2024. Curriculum is updated every 180 days. Additionally, audio, video, and digital content for printing is developed, distributed and added to the Primex^3 portal every 30 days.

Why is the NH-MCDP Universal? Although the partners, political environment, and degree of Home Rule vary greatly, any other State or Territory could duplicate this framework to improve the capabilities of tens of MILLIONS of Human Intrusion Prevention Systems across the NASCIO membership and work on a #1 NASCIO CIO Priority. The NH Municipal Cyber Defense Program is a cybersecurity training framework that consists of four pillars focused on the tens of thousands of Human Intrusion Prevention Systems in the Granite State: In-Person at Your Location Workshops, Live Webinar Training, In-Person Incident Response Planning and Exercises, Online Library of Micro-Trainings and Downloadable Content. **All NH MCDP services are provided at no cost to municipal and public sector entities and meet or exceed all security, privacy and accessibility requirements because that is simply the right thing to do!**

PART II: IMPLEMENTATION OF THE NH-MCDP

Roadmap: In August of 2022, three like-minded people sat down, broke bread, enjoyed a cigar and glass of bourbon (or two) and decided, "This is just unacceptable. We've got to do something to help mitigate these constant cyber incidents. We must figure out a way to accelerate cybersecurity readiness of the places we live, work, and raise our families – those [expletive deleted] don't get to win. Our biggest vulnerability is the user, and we need to transform them into 'Human Intrusion Prevention Systems' to help reduce the likelihood of these stupid human tricks'." The Group of Three knew the NH MCDP team needed to grow beyond three like-minded people and evolve into the primary vehicle for enhancing New Hampshire's Cybersecurity Readiness and creating a culture of security across the State.

Improving the Human Intrusion Prevention System Secures and Protects:

- The Three Branches of State Government and Local Governments' ability to deliver essential government services to residents, visitors, and businesses – Training and assessments are delivered in person or live online as requested by the Branches of the State Government, the Secretary of State, Cities, Towns, and Counties in New Hampshire.
- Local K12s' and the University System of New Hampshire's (USNH) ability to deliver seamless educational and counselling services while protecting staff and student privacy as well as sensitive research – Training and assessments are delivered in person at K12 schools and State Universities across the State.
- First Responders' ability to deliver emergency services within their jurisdictions and provide mutual aid as required – Training and assessments delivered in person at the PD and FD stations across New Hampshire.
- Public Sector Supervisory Control and Data Acquisition (SCADA) operators' ability to manage Drinking Water and Wastewater facilities – Training and assessments delivered in person at facilities across the State.
- Public trust in State and Local Government Organizations by providing comprehensive Cybersecurity training to New Hampshire residents – Delivered in Public Libraries in every region of New Hampshire – even where *Northwoods Law* is filmed!

After that initial meeting in August of 2022, the Group of Three began to codify the way ahead. They collaborated with a variety of stakeholders across Federal, State, and Local Government and determined that the most efficient way to improve the Human Intrusion Prevention Systems was to accelerate the assessments, training, and workshops provided by the NH MCDP.

They built a program that leverages federal grant funding to:

- Acknowledge that "Grifters were grifting, Phishers were phishing, and Clickers were clicking" but Human Intrusion Prevention Systems could be improved. **(Assumption)**
- Improve the capability and capacity of NH's Tens of Thousands of Human Intrusion Prevention Systems (HIPS) against cyber-attacks. **(Outcome)**
- Add value and not duplicate services or training that were already available. **(First Principle)**
- Analyze data to determine NH-specific gaps and needs for cybersecurity training. **(Activity)**
- Develop & Deliver Training based on this analysis. **(Activity)**
- Provide Conference & Group Training Sessions. **(Activity)**
- Provide Audio, Video, and Infographic Training Aids. **(Activity)**
- Ensure "significant training events" could be delivered as 90-minute, 2-hour, 4-hour, and full day workshops or via a webinar format. **(Activity)**
- Deliver Training at both the Primex[3] facility and "On Location Locally." **(Activity)**

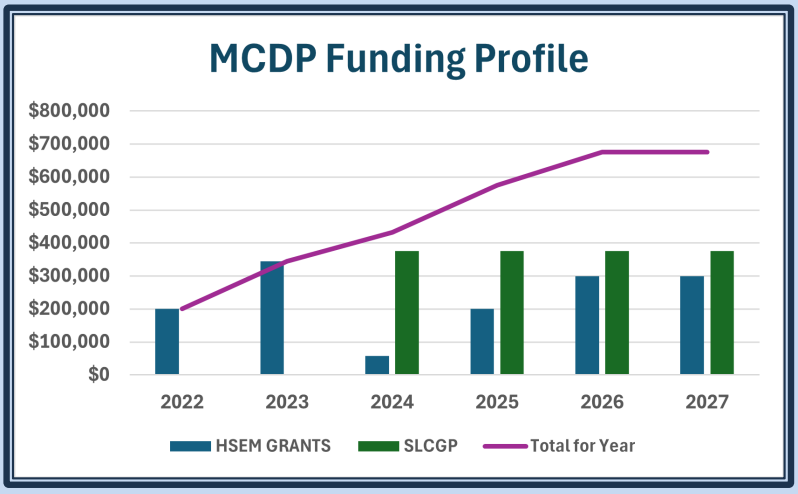
Who Was Involved – The Public-Private Partnership

- The OG "Group of Three": The Senior Partner of the Atom Group Security and Privacy Practice/Chairman of the Board of The Overwatch Foundation, the Lead Cybersecurity Risk Manager for the New Hampshire Public Risk Management Exchange (Primex^3) and the NH State Chief Information Security Officer (CISO).
- Primex^3 is a NH Not-For-Profit Public Entity Risk Pool that understands the needs of New Hampshire's cities, towns, school districts, counties, village districts, and other governmental entities, focusing exclusively on coverage to protect public sector entities. Primex^3 standards of organization and operation, as well as the coverages and services they are authorized to provide is codified in New Hampshire Revised Statute as Amended (RSA) Title I, The State and Its Government, Chapter 5-B, Pooled Risk Management Programs.
- The New Hampshire Municipal Association (NHMA) is a NH Not-For-Profit whose chartered purposes include: (a) provide technical assistance, information, advice, and other services to New Hampshire municipal officials to enable them to serve their municipalities more effectively; (b) improve the education and training of locally appointed and elected officials and employees; and (c) take advantage of any savings and improved administration that can be achieved through the pooled operation of services for members.
- The New Hampshire Department of Safety, Homeland Security and Emergency Management.
- The Atom Group, LLC is a local New Hampshire business with offices in Portsmouth and Concord. Atom is the Cyber Emergency Response Provider for Primex^3 and has contracts for similar services with the larger New Hampshire cities that are not Primex^3 members as well as the State of New Hampshire. Additionally, they are trusted partners of Major Insurers and the Major Legal Firms in New Hampshire that provide breach counselling services, and other Cyber related legal services. They are familiar, at the deepest technical levels of the IT environments used by municipal organizations across the State and those used by the State Government of New Hampshire.
- The New Hampshire Department of Information Technology and Office of the Chief Information Security Officer.
- Other significant collaborators on the NH-MCDP team include:
- The New Hampshire CTO Council, comprised of technology leaders from all 108 NH K12 School Administrative Units (SAU)
- The NH Municipal IT Directors Association
- The Overwatch Foundation, a NH Not-for-Profit with the mission to protect critical infrastructure, the New Hampshire competitive advantage, and the public trust by providing grant-funded cybersecurity auditing and engineering, infrastructure and software modernization, and workforce development.

Throughout this story, many NH organizations have been mentioned, but the chart on the left summarizes the organizations that formed the critical mass of the NH-MCDP Public-Private Partnership.

As you probably know, the Granite State is smaller than most, and we had the benefit of leveraging both personal and professional pre-existing trust relationships across all these organizations and State Agencies, we even consider our NH CISA Cyber Advisor a "local." We already socialize with each other!

How did we do it? The program is entirely funded by the NH Department of Information Technology through Homeland Security Grants, the State and Local Cybersecurity Grant Program (SLCGP), and by Primex^3 funds allocated to training facilities and the Primex^3 Online Training Portal for their members. Near the end of 2022, the acceleration of training for Human Intrusion Prevention Systems began with a "repurposed" $190K HSEM Grant. Atom Group hired and dedicated 1 full time staff for organization and scheduling and leveraged the additional funding to pay for existing employees to develop and deliver addition content. Over the next two years, additional HSEM Grants and the State and Local Cybersecurity Grant Program were leveraged to increase and sustain funding for the program.



NH-MCDP TRAINING FOR HUMAN INTRUSION PREVENTION SYSTEMS

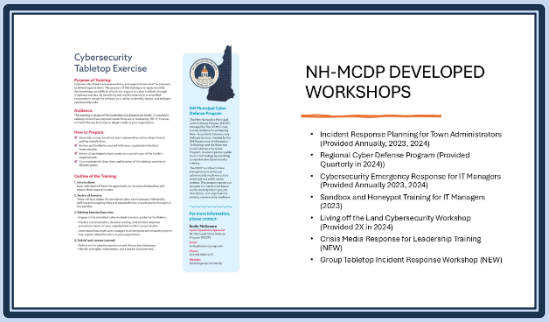
- **General Cybersecurity Awareness Training**
- **Public Cybersecurity Training for Libraries**
- **Cybersecurity Training for Police and Fire Departments**
- **Cybersecurity Training for Financial Teams**
- **Cybersecurity Training for IT Teams**
- **How to Legally Review Cybersecurity Documentation and Policies**
- **Cybersecurity Incident Response Plan Creation**
- **Tabletop Workshop for cybersecurity incident response plans**
- **Cybersecurity Microsoft O365 Secure Setup Review and Training**
- **Cybersecurity Training for Educators (K-12 & SAU)**
- **Cybersecurity Voting Protection Training for Cities and Towns**
- **Cybersecurity Advanced Indicator of Compromise Detection Training (For IT Engineers)**
- **Data Privacy Training for Emergency Responders.**
- **CIS Controls Webinar Series (Controls 1-16, Implementation Group 1&2)**
- **Region Cyber Defense Training Program**

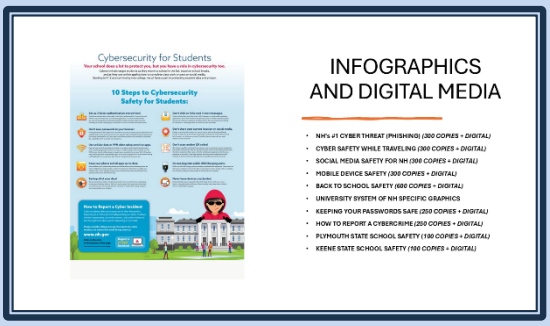
TRAINING IN PURPLE WAS CREATED AS PART OF NH-MCDP EXPANSION.

From 2023 to 2024, additional data was collected by Primex^3, The Atom Group, and the NH CISA Cyber advisor that informed the development of eleven new major training curricula for delivery through the NH MCDP. Each of these sessions were designed with intention to correct trending mistakes by the tens of thousands of Human Intrusion Prevention Systems using, operating and maintaining State and Local Information Systems to deliver essential Government Services.

Many of these programs are also delivered in large group settings and are always open to the public. Certain sessions, such as the Regional Cyber Defense Training Program are also open to IT Managed Service Providers that have contracts with Cities and Towns throughout New Hampshire. The more brains we have trying to mitigate this problem, the better! We've even done combined sessions for New Hampshire and Vermont where it makes sense!

PART III: Impact of the NH-MCDP on Human Intrusion Prevention Systems





What Did We Make Better? As in most states, there are a variety of conferences throughout the year. The NH MCDP has revolutionized Cybersecurity discussions at these events. We've reached thousands of Civic Leaders, Elected Officials, School Administrators, and Police and Fire Chiefs over the last two years at their conferences with MCDP workshops. We have "reserved spots" for NH MCDP training at the annual meeting of the New Hampshire Municipal Association, The NH PRIMEX Annual Meeting, The New Hampshire Digital Government Summit, The Association of Counties Annual Meeting, Quarterly K12 CTO Association meetings, Quarterly Municipal IT Directors meetings, annually for the NH Cybersecurity Advisory Committee, annually on the Legislative Branch's Organizational Day at the beginning of the session and quarterly at both the NH Associations of Police and Fire Chiefs. NH MCDP trains thousands of Human Intrusion Prevention Systems annually. MCDP Infographics are displayed in hundreds of public facilities around the state.

"The most useful training I've ever had on Cybersecurity in my 24 years as a Fireman and in my time as Chief. Every time one of my Firefighters does NOT click, it ensures we can answer that next call from dispatch."

-Chief, Durham, NH/University of New Hampshire Fire Department
Training Critique, June 2023

"Based on two years of Primex[3] Claims data, each claim costs about $10K on average just for incident response. That doesn't even come close to the costs to remediate and rebuild after a Ransomware incident. That can be and has been millions. Primex[3] members clicking on Phishing emails start it all. Millions of dollars are saved if that doesn't happen."

- Ken Weeks, CISO, State of New Hampshire.

How Do We Know We Succeeded?

Since early 2023, the MCDP has provided training to more than 7,000 Human Intrusion Prevention Systems. Training has been used by 40% (4 of 10) of NH Counties, 46% (6 of 13) of NH Cities, 17% (37 of 221) of NH Towns, 40% (56 of 139) of the SAUs and 18% of NH First Responders. (In many cases engagements with Cities/Towns and their Police and Fire Departments are coordinated or integrated.) This is an impressive service rate and return on the investment over the first 2.5 years of the program!

According to the latest Verizon Data Breach Investigations Report (DBIR) the National click average on Phishing emails in 2022 was well over 10% and it takes a clicker less than 21 seconds to decide to click. In 2022, based on more limited data, the New Hampshire Public Sector click rate was approximately 7.4%. Since the acceleration of the NH MCDP training, measurable public sector click rates across New Hampshire in 2024 are down to 3.2%. **Awareness results in a pause. A pause results in a question. A user chooses not to click and chooses to report. Improvement was just made to the NH Culture of Security.**

From an Email dated 1/22/2024:

Good news regarding schools engaging with the MCDP training program. As you know, Hollis Brookline School districts lead the charge in requiring MCDP Cybersecurity training for all district educators, staff, and administrators. We reached a massive set of over 300+ people across those districts.

Lately, other districts have been picking up the charge and continuing this trend, including New London, Sunapee, and Newington. The attendance and size of these trainings are now well over 100 people in person and have been over 250+ in some cases. We're pleased with this growth. This is on top of significant growth in the engagement with the towns and other target areas.

As an example, Cheshire County just completed a three-phase training session for the Nursing Home, General Finance Staff, and County Jail staff, which delivered unique training for cyber risk inside of those environments as part an all-day cyber program.

While demand has been high since the inception of the MCDP, we're seeing increasingly strong engagement, and the number of people we reach per dollar is trending upward quickly.

Best,
Jason
Jason J. Sgro
Senior Partner, Atom Group

What Now?

Planned and funded growth areas for the MCDP are:

- "Cybersecurity Training for NH Residents" at Public Libraries across the State (17 have been provided)
- "Cybersecurity training for SCADA Operators" at NH Drinking Water and Wastewater systems (17 sessions have been provided)
- "Social Media, Travel, and Mobile Device Safety" for K12 Students (High School Sessions Piloted)
- "Cybersecurity and Safety for Students – School Assembly in the Gym or Theater Version"

As of today, the NH MCDP has a 7-month backlog of training requests. Atom Group has hired an additional full-time trainer and another part-time trainer to close this gap. As you can see in the email to the left, demand is soaring, but the number of Human Intrusion Prevention Systems trained per dollar spent is trending upward!

By educating and training the Human Intrusion Prevention Systems (HIPS) across the State of New Hampshire, the NH MCDP is building a Culture of Security at all levels of Government and with NH Residents. The program is directly contributing to the number of "pauses before clicking" and preventing cybersecurity incidents. By leveraging cross-boundary collaboration and partnerships, New Hampshire is actively fighting back to protect our way of life by making it more difficult for Malicious Cyber Actors to achieve their objectives. **Going back to where it all started and as the original group of three said, "…those [expletive deleted] don't get to win."**

NH CYBER DEFENSE PROGRAM
POWERED BY ATOM

SEAL OF THE STATE OF NEW HAMPSHIRE
1776

Live Free or Die!