NEWTON PUBLIC SCHOOLS
Equity & Excellence

To: Newton Public Schools School Committee
From: Steven Rattendi, Director of Information Technology and Library Services
Date: Friday, December 2, 2022
Subject: December 5 Cybersecurity Update

Attached are materials for the December 5 Cybersecurity Update. This presentation will provide a high-level overview of the framework we use for Cybersecurity in the Newton Public Schools and a few sample items of work we currently do and hope to do this year and in the coming years.

As part of our 2022-2023 District Wide Goals we have the following objective and action steps related to cybersecurity:

> *Strengthen procedures and methods to maintain data security*
> - *Continue to Improve network systems, servers, and software to maintain data security.*
> - *Continue to educate staff on best practices for data security.*
> - *Assess the need for and implement additional security procedures including 2-factor authentication.*

Our Cybersecurity posture is defined by practices in the education industry, our partnership with the City of Newton IT Department, information from our partner vendors, and national agencies such as the US government's *Cybersecurity and Infrastructure Security Agency (CISA)* and the *National Institute of Standards and Technology*. Educational institutions are not unique in having to balance access with security, though we are unique in the sheer number of individuals (students, staff, and families) that need varying levels of access. Overly burdensome security can negatively impact the educational environment and access to learning materials, and, yet, schools' increasing reliance on technology requires a cyber environment that is not easily disrupted or exploited.

I will also be joining you, along with a few members of the ITLS (Information Technology and Library Services) team during Executive Session at 5:30 p.m. to answer more specific questions related to cybersecurity and cyber safety. The Executive Session will allow for a more open conversation without inadvertently revealing sensitive technical specifications.

Also attached is additional information on the CISA services we are making use of or hope to make use of this year along with a description of our newly formed NPS Cybersecurity Team.

Thank you and I look forward to our conversation on December 5.

NEWTON PUBLIC SCHOOLS
Equity & Excellence

NPS Cybersecurity Team

The NPS Cybersecurity Team was formed this school year (2022-2023). Below is an outline of the team's purpose, make-up, and tasks for this school year. The work of the NPS Cybersecurity Team will mimic much of the work of the district-wide NPS Safety Team which addresses issues related to the physical safety of students and staff.

Purpose

- Inform district policies and procedures related to cybersecurity
- Provide a wide-enough representation to inform cybersecurity needs in the district
- Act as a response team in the event of a district cybersecurity incident
- Discuss / Reflect on Cyberincidents as they occur

Members

Julie Athanansiadis, Business, Finance & Planning
Donna Benoit, NPS Career & Tech Ed, NESA
Eddie Earnest, IT & Library Services - Technical Support Services
Peter Hamel, NNHS Teacher, IT & Library Services - Instructional Technology
Caitlyn Hogue, Business, Finance & Planning
Joe Lamarca, IT & Library Services - Network Services
Samuel Mayanja, IT & Library Services - Network Services
John McLauglin, IT & Library Services - Network Services
Amy Mistrot, Business, Finance & Planning
Jack Polnar, IT & Library Services - Database Services
Steven Rattendi, IT & Library Services
Sue Riley, Health/Human Services, School Nursing
Jennifer Roy, IT & Library Services - Instructional Technology
Carol Stockdale, IT & Library Services, NESA

Members still to be recruited:
Human Resources, Student Services, City IT

Work Items (in development)

For 2022-2023	In the coming years
• 2-Factor Authentication Implementation • Cybersecurity Incident Response Plan • Assessment of End-User Practices	• End-user Training • Reviewing procedures related to Cybersecurity (timelines, equipment disposal practices, account management practices, etc.)

NEWTON PUBLIC SCHOOLS
Equity & Excellence

Cybersecurity Scanning

Description of CISA Services

From https://www.cisa.gov/cyber-resource-hub:

> *The Cybersecurity and Infrastructure Security Agency offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional, no-cost assessments are provided upon request on a voluntary basis and can help any organization with managing risk and strengthening the cybersecurity of our Nation's critical infrastructure.*

These services are offered at no cost to federal, state, local, tribal, and territorial governments, critical infrastructure, and federal agency partners. The services are provided on an as-available basis with consideration for priority industries and functions.

In September of 2022, Newton Public Schools applied to participate in the following CISA offerings:

- **Cyber Hygiene Vulnerability Scanning** is a persistent scanning service of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.
- **Web Application Scanning** evaluates known and discovered publicly-accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- **Remote Penetration Testing** focuses on testing a stakeholder's internet exposure.
- **Risk and Vulnerability Assessments** combine national threat information with data collected and vulnerabilities identified through on-site assessment activities to provide tailored risk analysis reports.

We have already begun to receive reports from the first two scanning items above (Cyber Hygiene Vulnerability Scanning and Web Application Scanning). We are waiting to hear about a timeline for the other two items.

NEWTON PUBLIC SCHOOLS
Equity & Excellence

NPS Cybersecurity Team

The NPS Cybersecurity Team was formed this school year (2022-2023). Below is an outline of the team's purpose, makeup, and tasks for this school year. The work of the NPS Cybersecurity Team will mimic much of the work of the district-wide NPS Safety Team which addresses issues related to the physical safety of students and staff.

Purpose

- Inform district policies and procedures related to cybersecurity
- Provide a wide-enough representation to inform cybersecurity needs in the district
- Act as a response team in the event of a district cybersecurity incident
- Discuss / Reflect on Cyberincidents as they occur

Members

Julie Athanansiadis, Business, Finance & Planning
Donna Benoit, NPS Career & Tech Ed, NESA
Eddie Earnest, IT & Library Services - Technical Support Services
Peter Hamel, NNHS Teacher, IT & Library Services - Instructional Technology
Caitlin Hogue, Business, Finance & Planning
Joe Lamarca, IT & Library Services - Network Services
Samuel Mayanja, IT & Library Services - Network Services
John McLauglin, IT & Library Services - Network Services
Amy Mistrot, Business, Finance & Planning
Jack Polnar, IT & Library Services - Database Services
Steven Rattendi, IT & Library Services
Sue Riley, Health/Human Services, School Nursing
Jennifer Roy, IT & Library Services - Instructional Technology
Carol Stockdale, IT & Library Services, NESA

Members still to be recruited:
Human Resources, Student Services, City IT

Work Items (in development)

For 2022-2023	In the coming years
• 2-Factor Authentication Implementation • Cybersecurity Incident Response Plan • Assessment of End-User Practices	• End-user Training • Reviewing procedures related to Cybersecurity (timelines, equipment disposal practices, account management practices, etc.)

Cybersecurity Overview

School Committee, December 5, 2022
NPS IT & Library Services Department

NEWTON
PUBLIC SCHOOLS
Equity & Excellence

Presentation Overview

- District wide goal
- Importance
- Cybersecurity framework
- Broad overview of current work
- Challenges

District Goal

Strengthen procedures and methods to maintain data security

- Continue to enhance network systems, servers, and software to maintain data security.
- Continue to educate staff on best-practices for data security.
- Assess the need for and implement additional security procedures including 2-factor authentication.

Why is Cybersecurity Important?

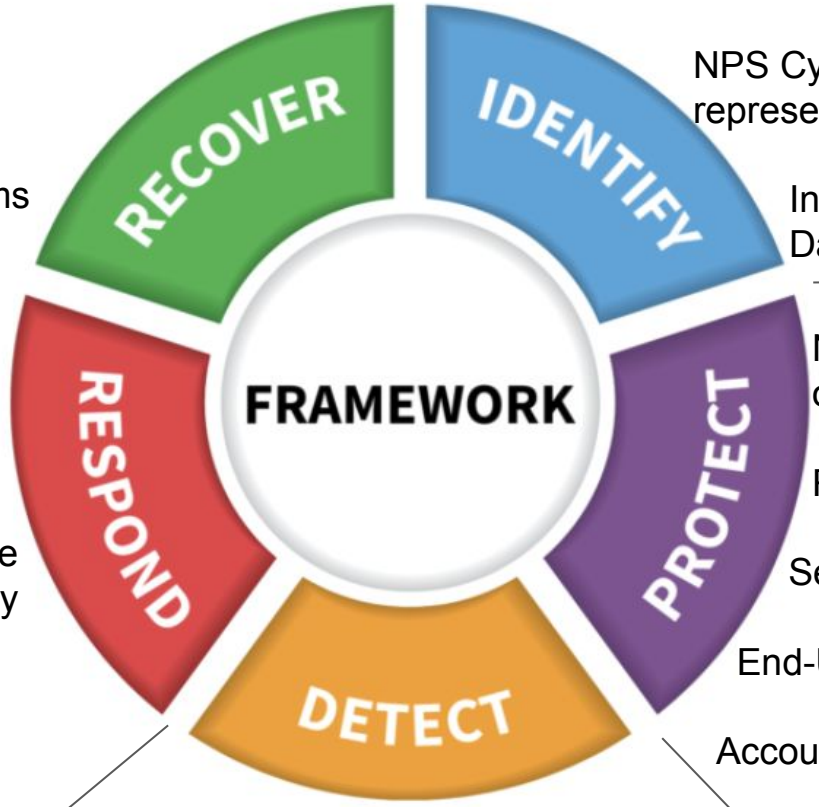
- We process and hold a large amount of data on:
  - Students
  - Employees
  - Graduates
- Governments and Schools have increasingly become targets of Cyber Breaches and they are disruptive
  - In 2021 there were 166 publicly disclosed school cyber incidents nationwide according to the K-12 Security Information Exchange (K-12 SIX)
  - Sept 2022: Los Angeles Unified School District experience a ransomware attack
  - Sept 2022: Michigan South Redford School District shut for 2 days
  - October 2020: Springfield Public Schools, MA, shutdown
  - Sept 2020: Hartford Public Schools, CT delayed opening of schools

Cybersecurity Framework

The next few slides will outline in broad strokes some of the things that fall under these categories that we do and are looking to do.

Cybersecurity Framework from National Institute of Standards and Technology, U.S. Department of Commerce

A Sampling of Current Work



Scanning Reports from US Government's Cybersecurity and Infrastructure Security Agency

NPS Cybersecurity Team with representatives from various departments

Internal Documentation of Servers, Data Storage, Cloud Systems

Network Firewalls / DNS Scanning, other Infrastructure

Regularly patching/updating systems

Segregated Network Structures

End-User Behavior / Training

Account Audits

Data Privacy Agreements / Software Vetting

Virus/Malware Scanning
Gmail Alerts for possible Impersonation emails
Hardware Reports / User Reports

Work to build knowledge redundancy

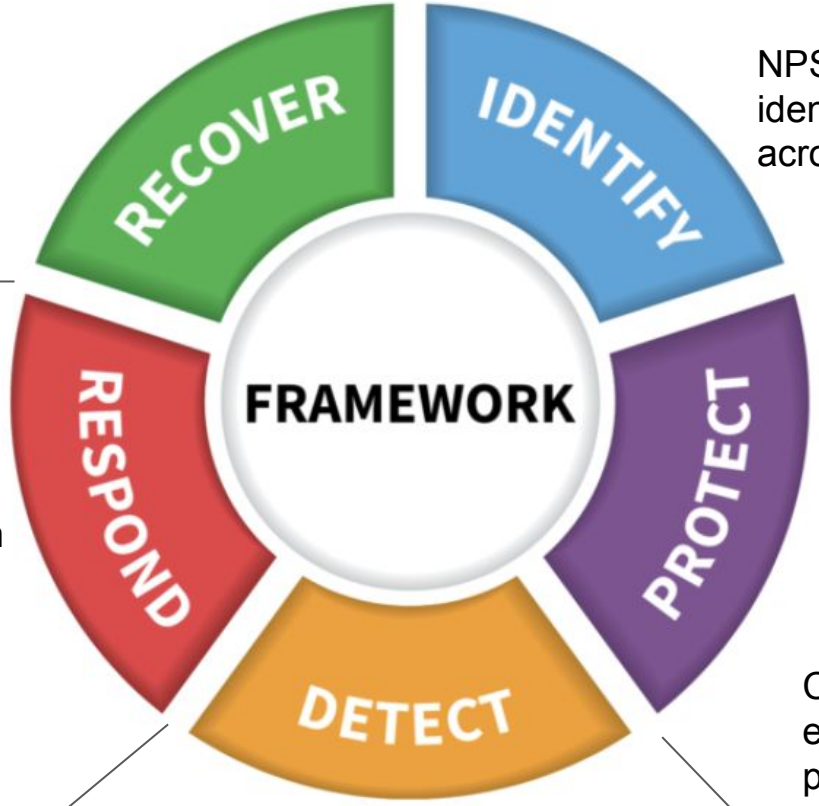
IT Staff knowledge of systems

Multiple Points of Egress to the Internet

Data Backup Systems

A Sampling of Work to be Done

Additional Services from US Government's Cybersecurity and Infrastructure Security Agency



NPS Cybersecurity Team to continue to identify processes for Data Security across various departments

Formalize internal Cybersecurity practices in a timeline for the year

Re-examine Policies/Guidelines (Student/Employee AUP/AUG, Web Publishing

Implement 2-Factor Authentication

Formalize a Cyber Incident Response Plan (NPS Cybersecurity Team)

Continue to offer and enhance end-user training including best practices for sharing within Google Docs / update annual training as part of HR training materials

Challenges

- We have MANY district users - keeping up with high quality training and the time to implement the training is a challenge
- Balance of ACCESS and SECURITY
- Keeping up with system upgrades
  - Updates are rarely a “one and done” scenario
  - Updates sometimes have ripple effects on functionality of other systems / software
- Resource limits and balancing priorities
- We don’t know what we don’t know - cybersecurity consultant