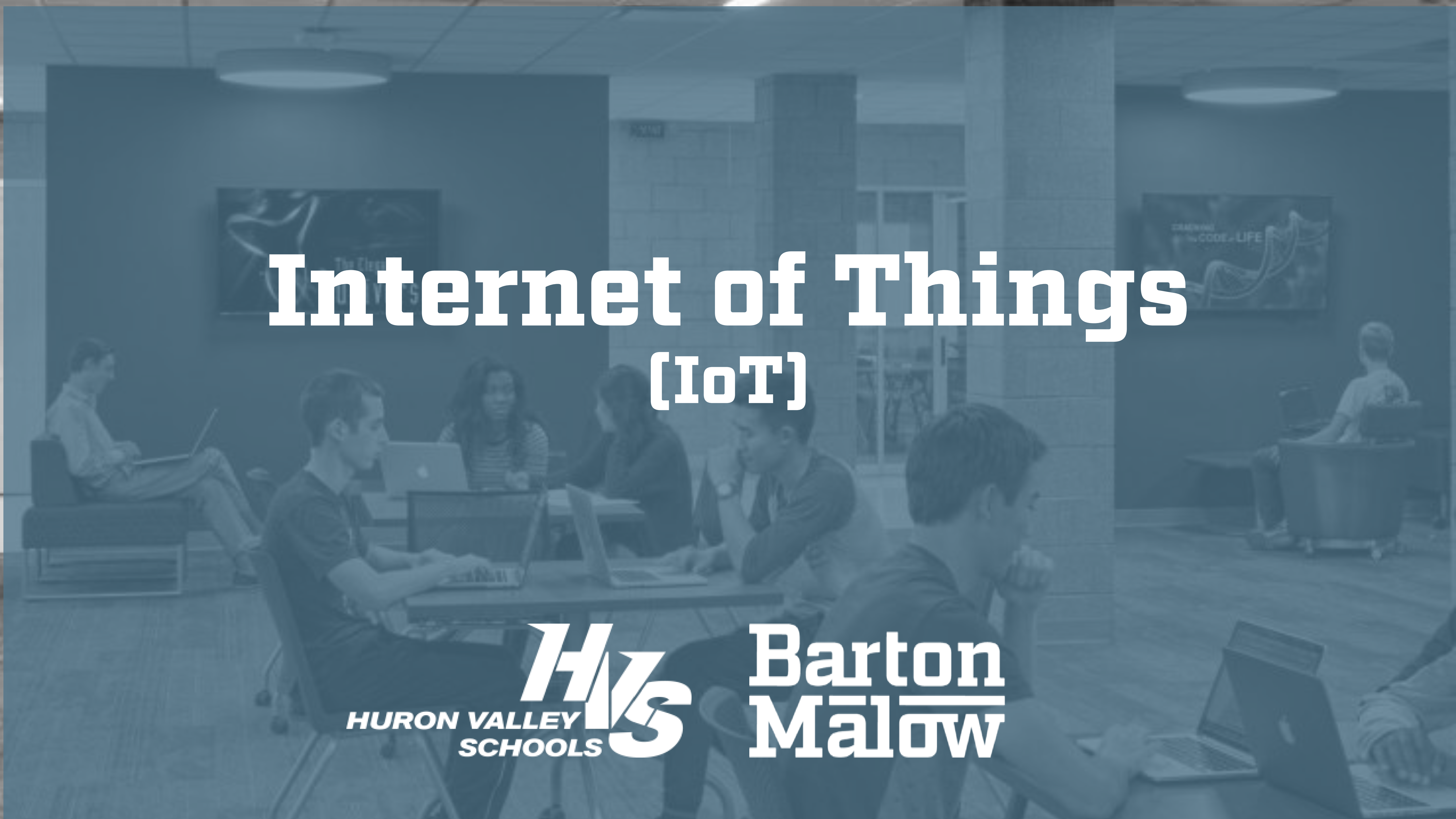
Funding Opportunities for IT Security

HURON VALLEY SCHOOLS

Barton Malow



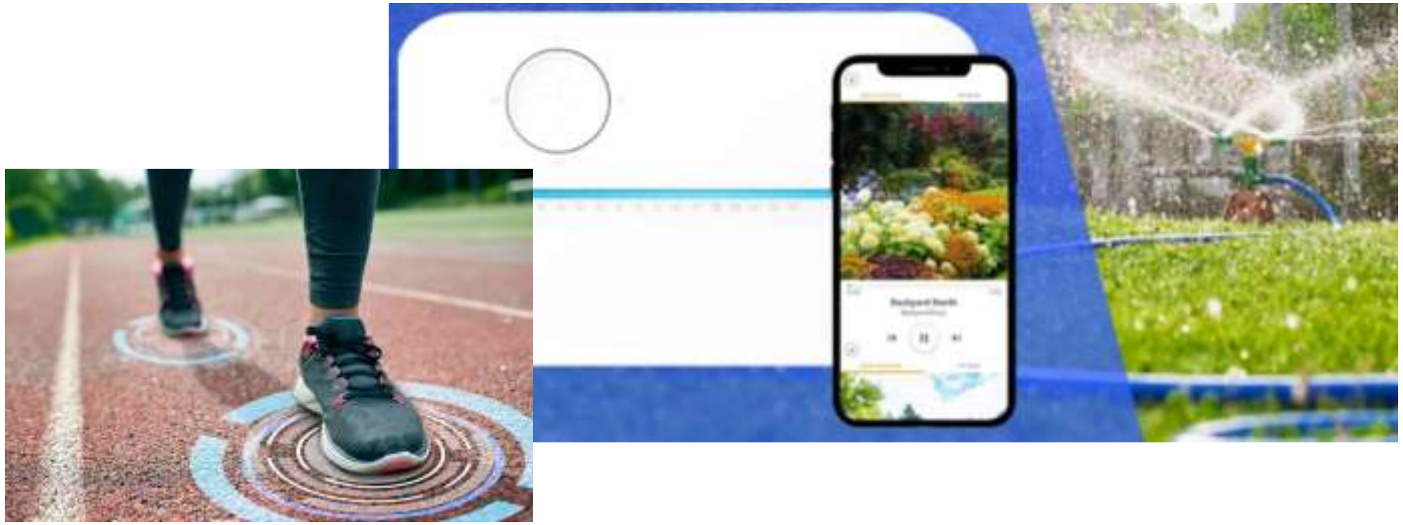
Internet of Things

(IoT)

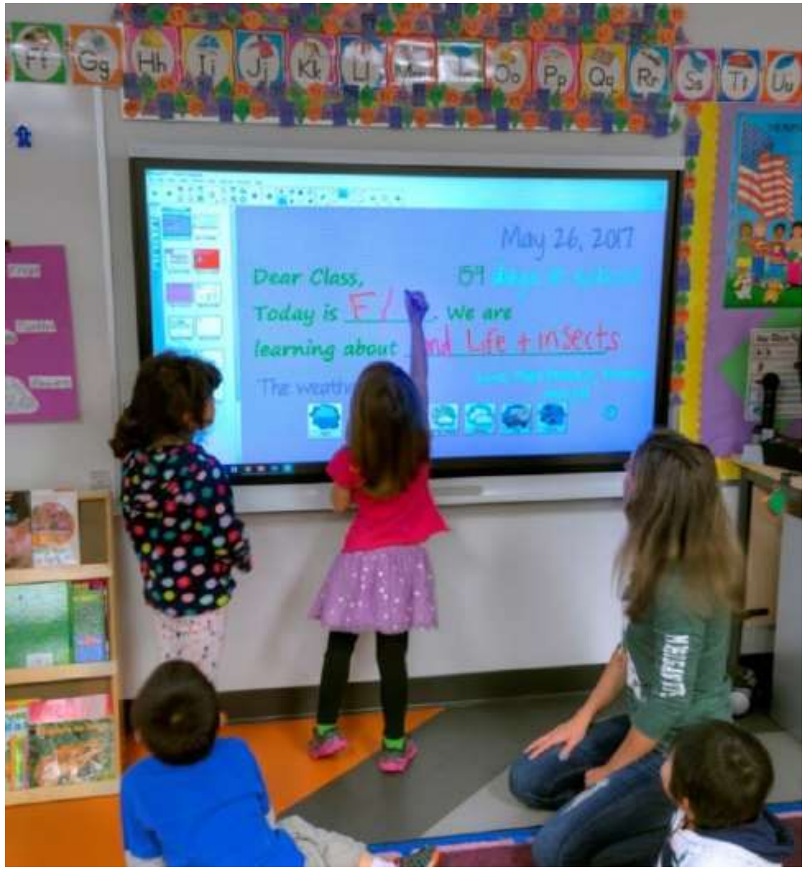
HURON VALLEY SCHOOLS

Barton Malow

IoT at Home



IoT at Home – Really?



IoT at School

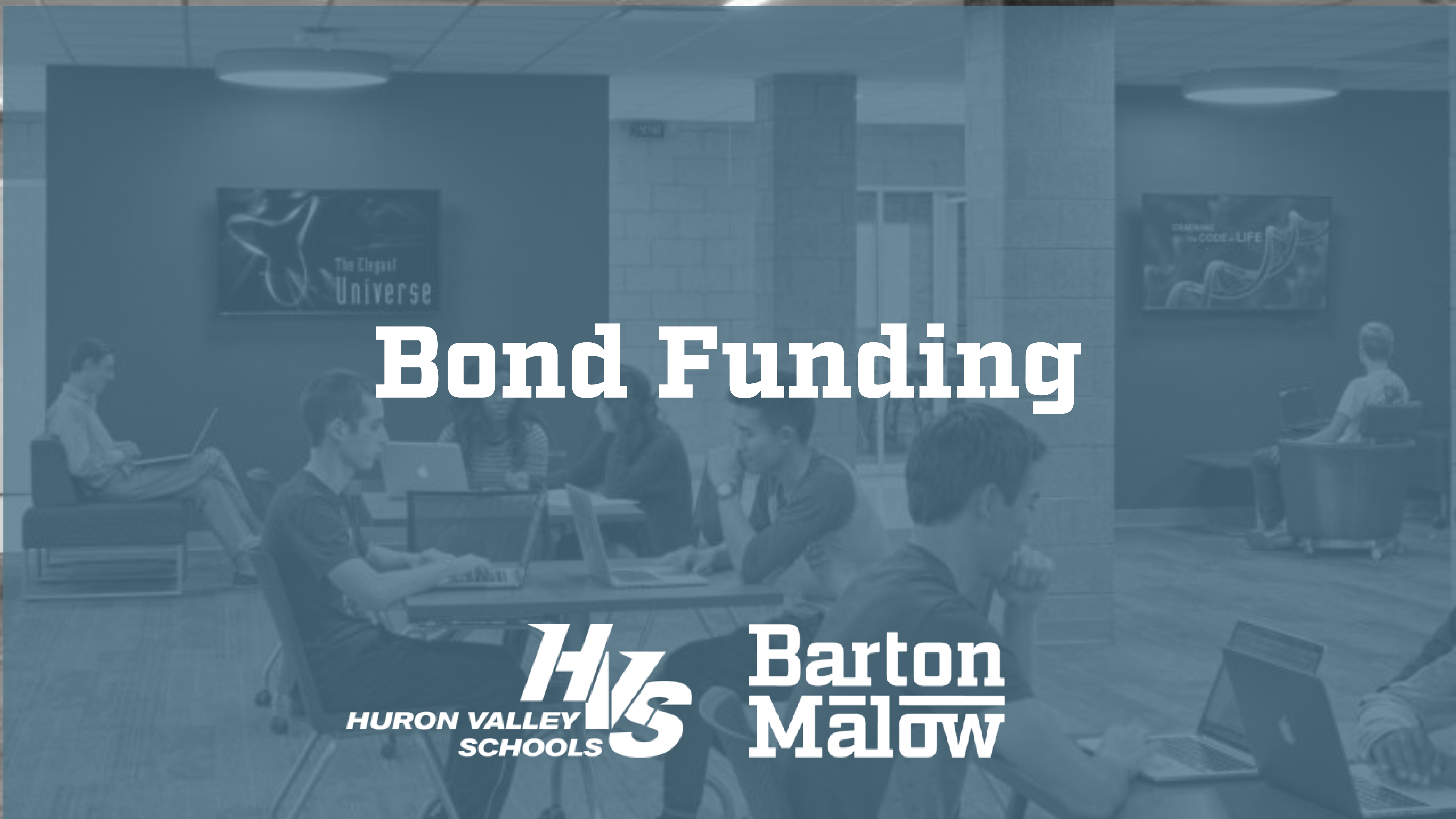
HURON VALLEY SCHOOLS

Barton Malow

IoT at School

HURON VALLEY SCHOOLS HVS

Barton Malow



Bond Funding

HVS
HURON VALLEY
SCHOOLS

Barton
Malow

IoT at School

HURON VALLEY SCHOOLS

Barton Malow

HURON VALLEY SCHOOLS

Barton Malow

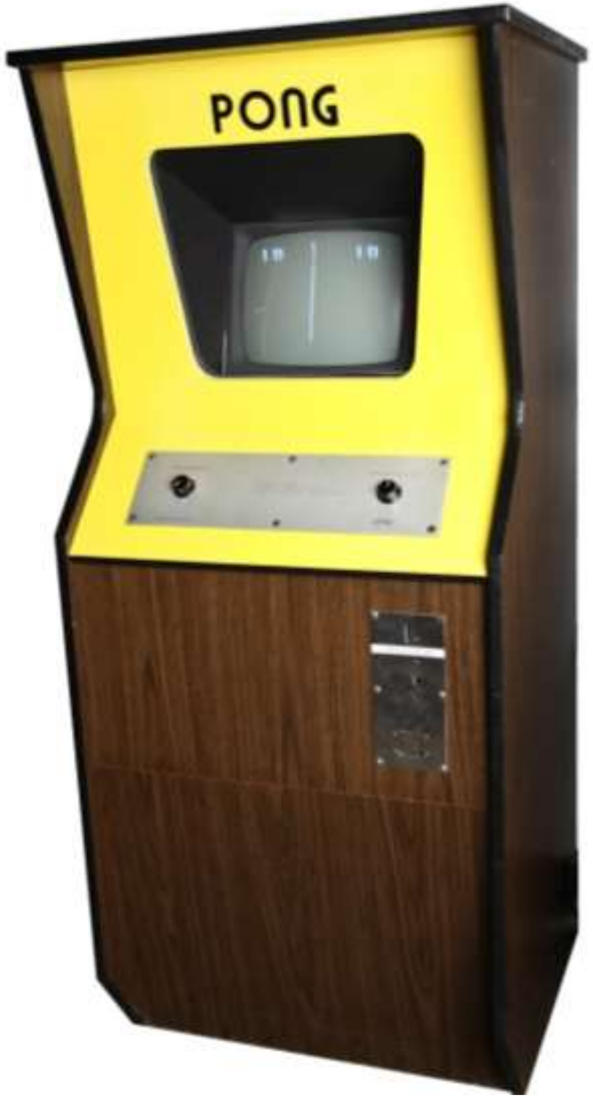
What Happened In… 1976

Drops out of Harvard

Apple Founded

IBM Invents the Floppy Disk

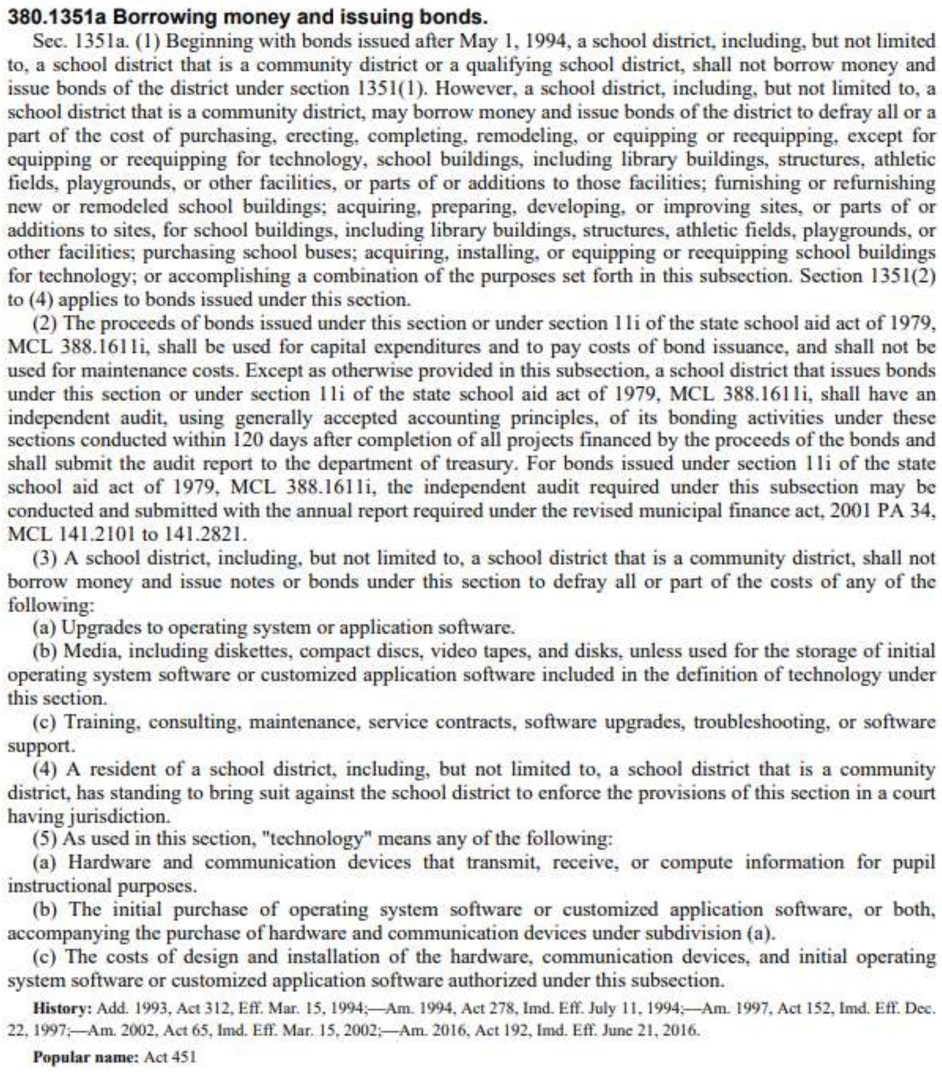
What Happened In… 1976



Atari 2600

(Not 'til 1977)

The Revised School Code - Act 451 of 1976



380.1351a Borrowing money and issuing bonds.

Sec. 1351a. (1) Beginning with bonds issued after May 1, 1994, a school district, including, but not limited to, a school district that is a community district or a qualifying school district, shall not borrow money and issue bonds of the district under section 1351(1). However, a school district, including, but not limited to, a school district that is a community district, may borrow money and issue bonds of the district to defray all or a part of the cost of purchasing, erecting, completing, remodeling, or equipping or reequipping, except for equipping or reequipping for technology, school buildings, including library buildings, structures, athletic fields, playgrounds, or other facilities, or parts of or additions to those facilities; furnishing or refurnishing new or remodeled school buildings; acquiring, preparing, developing, or improving sites, or parts of or additions to sites, for school buildings, including library buildings, structures, athletic fields, playgrounds, or other facilities; purchasing school buses; acquiring, installing, or equipping or reequipping school buildings for technology; or accomplishing a combination of the purposes set forth in this subsection. Section 1351(2) to (4) applies to bonds issued under this section.

(2) The proceeds of bonds issued under this section or under section 11i of the state school aid act of 1979, MCL 388.1611i, shall be used for capital expenditures and to pay costs of bond issuance, and shall not be used for maintenance costs. Except as otherwise provided in this subsection, a school district that issues bonds under this section or under section 11i of the state school aid act of 1979, MCL 388.1611i, shall have an independent audit, using generally accepted accounting principles, of its bonding activities under these sections conducted within 120 days after completion of all projects financed by the proceeds of the bonds and shall submit the audit report to the department of treasury. For bonds issued under section 11i of the state school aid act of 1979, MCL 388.1611i, the independent audit required under this subsection may be conducted and submitted with the annual report required under the revised municipal finance act, 2001 PA 34, MCL 141.2101 to 141.2821.

(3) A school district, including, but not limited to, a school district that is a community district, shall not borrow money and issue notes or bonds under this section to defray all or part of the costs of any of the following:

(a) Upgrades to operating system or application software.

(b) Media, including diskettes, compact discs, video tapes, and disks, unless used for the storage of initial operating system software or customized application software included in the definition of technology under this section.

(c) Training, consulting, maintenance, service contracts, software upgrades, troubleshooting, or software support.

(4) A resident of a school district, including, but not limited to, a school district that is a community district, has standing to bring suit against the school district to enforce the provisions of this section in a court having jurisdiction.

(5) As used in this section, "technology" means any of the following:

(a) Hardware and communication devices that transmit, receive, or compute information for pupil instructional purposes.

(b) The initial purchase of operating system software or customized application software, or both, accompanying the purchase of hardware and communication devices under subdivision (a).

(c) The costs of design and installation of the hardware, communication devices, and initial operating system software or customized application software authorized under this subsection.

History: Add. 1993, Act 312, Eff. Mar. 15, 1994;—Am. 1994, Act 278, Imd. Eff. July 11, 1994;—Am. 1997, Act 152, Imd. Eff. Dec. 22, 1997;—Am. 2002, Act 65, Imd. Eff. Mar. 15, 2002;—Am. 2016, Act 192, Imd. Eff. June 21, 2016.

Popular name: Act 451

380.1351a Borrowing money and issuing bonds

(3) A school district, including, but not limited to, a school district that is a community district, **shall not borrow money** and issue notes or bonds under this section to defray all or part of the costs of any of the following:

(c) Training, **consulting**, maintenance, service contracts, software upgrades, troubleshooting, or software support

State and Local Cybersecurity Grant Program (SLCGP)

HURON VALLEY SCHOOLS

Barton Malow

State & Local Cybersecurity Grant Program (SLCGP)

History

- Included in the Infrastructure Investment and Jobs Act (IIJA) of 2021
  - $1B over 4 years with $185M allocated in 2022
  - 56 U.S. states and territories could apply by November 15, 2022
- States formed Cybersecurity Planning Committees to Apply
  - State, County and Local Representatives
  - Public Education
  - Public Health
  - Rural, Suburban and High-Population
- Required a Cybersecurity Plan

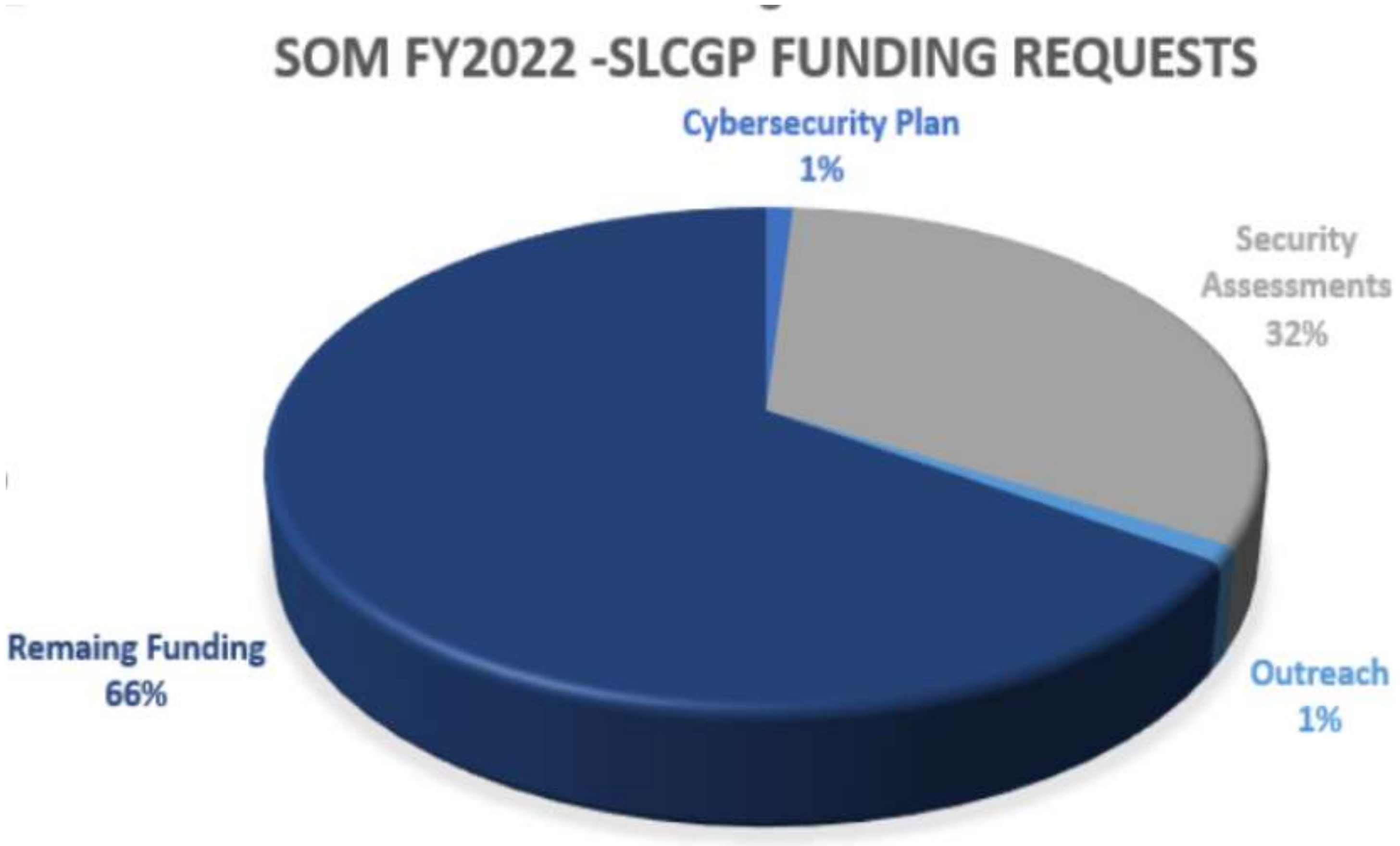
State & Local Cybersecurity Grant Program (SLCGP)

Estimated Grant Allocation

- FY22 - $185 Million | Match 10 Percent
- FY23 - $400 Million | Match 20 Percent
- FY24 - $300 Million | Match 30 Percent
- FY25 - $100 Million | Match 40 Percent

- Sub-grant award recipients must provide funding match at project level.
- Amount is calculated by a formula based on the amount requested
- 80% of funds to local governments, with minimum 25% to rural areas

Information From DTMB



SOM Grant Funds
FY2022 Funds
$4,775,415 Awarded
$1,650,000 Requested in Application for Projects Supporting Development of The Cybersecurity Plan
FY2022 Remaining $3,125,415
Local Project Requests must be able to provide matching funding at the project level to be supported.

Requirements for Grant Funding Use

Cannot Use Grant Funds For:

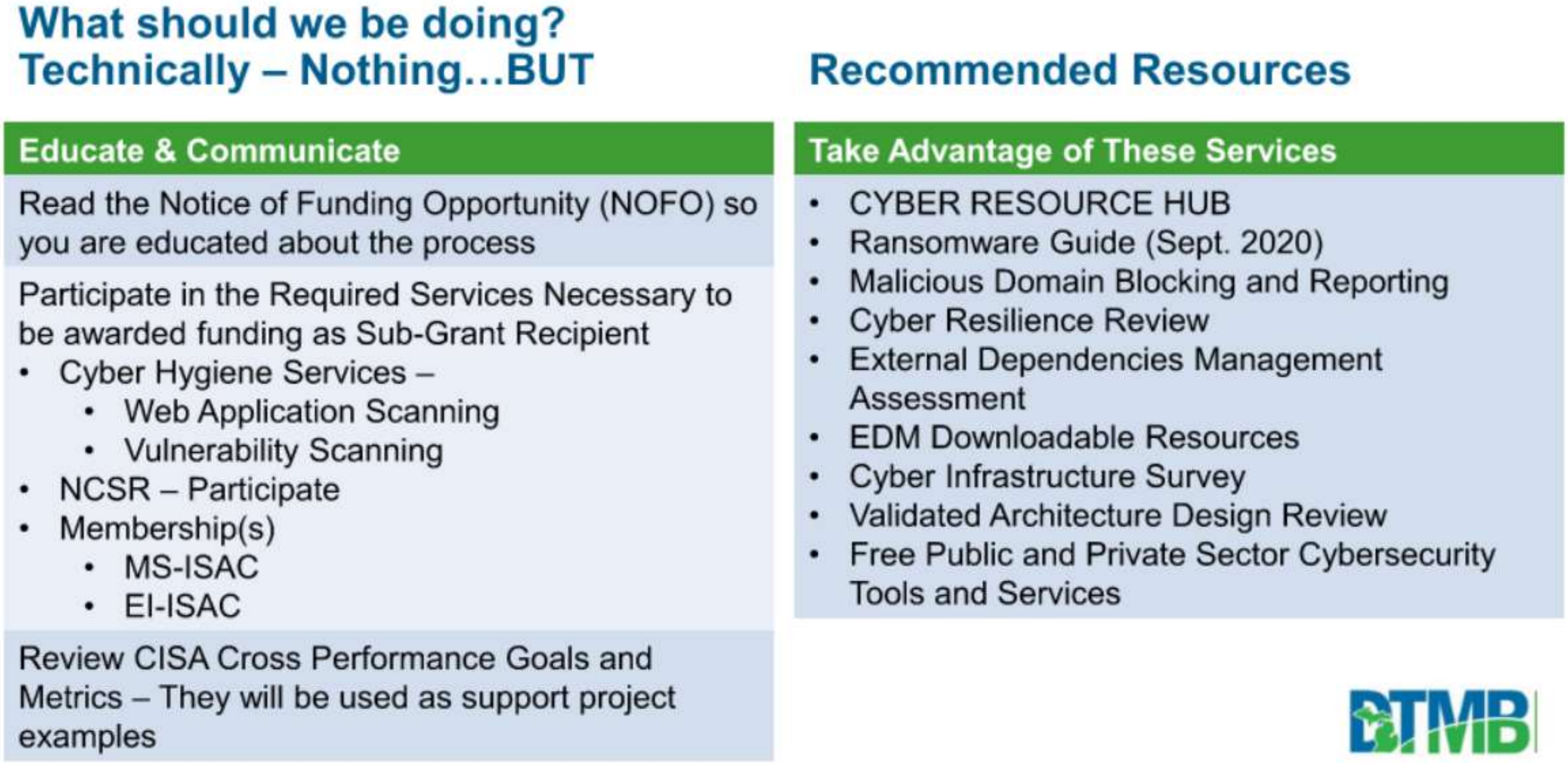
- Supplanting other state or local funds
- The substitution of recipient cost-sharing contributions
- Payment of a ransom from cyberattacks
- Recreational or social purposes, or for any purpose that does not address cybersecurity risks or cybersecurity threats on SLTT information systems
- Lobbying or intervention in federal regulatory or adjudicatory proceedings
- Suing the federal government or any other government entity
- Acquiring land or constructing, remodeling, or altering buildings or other physical facilities
- Cybersecurity insurance
- Any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity or local government within the jurisdiction of the eligible entity.

Michigan Status

- October 19, 2022: 23-member Cybersecurity Planning Committee formed
- November 15, 2022: All 56 entities submitted applications
- 53 of 56 applications have been reviewed
- December 19, 2022: Michigan's grant application was approved with an exception
  Michigan must submit a complete cybersecurity plan
- **September 2023: Cybersecurity Plan deadline**

No current action required for local entities to be eligible subrecipients

DTMB Information



What should we be doing?
Technically – Nothing…BUT

Educate & Communicate

Read the Notice of Funding Opportunity (NOFO) so you are educated about the process

Participate in the Required Services Necessary to be awarded funding as Sub-Grant Recipient

- Cyber Hygiene Services –
  - Web Application Scanning
  - Vulnerability Scanning
- NCSR – Participate
- Membership(s)
  - MS-ISAC
  - EI-ISAC

Review CISA Cross Performance Goals and Metrics – They will be used as support project examples

Recommended Resources

Take Advantage of These Services

- CYBER RESOURCE HUB
- Ransomware Guide (Sept. 2020)
- Malicious Domain Blocking and Reporting
- Cyber Resilience Review
- External Dependencies Management Assessment
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Validated Architecture Design Review
- Free Public and Private Sector Cybersecurity Tools and Services

Resources

Michigan Cyber Partners

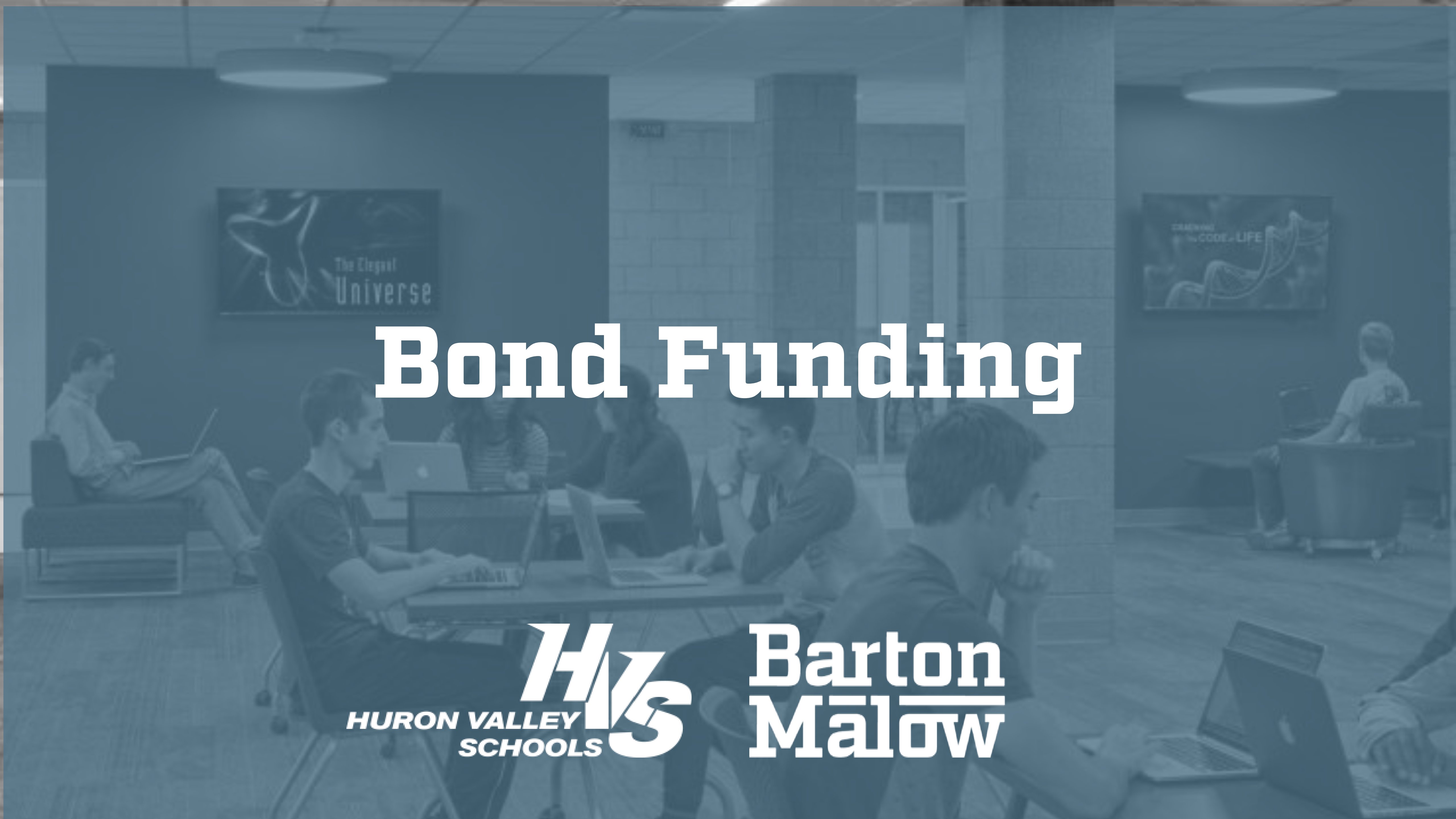
https://www.michigan.gov/dtmb/services/cybersecurity/cyber-partners

Michigan SLCGP Grant Contacts

dtmb-cyberpartners@michigan.gov

MiDEAL Cyber Assessments

https://www.michigan.gov/dtmb/services/cybersecurity/cyber-partners/prevent/resources/pre-approved-vendors-for-independent-cyber-assessment

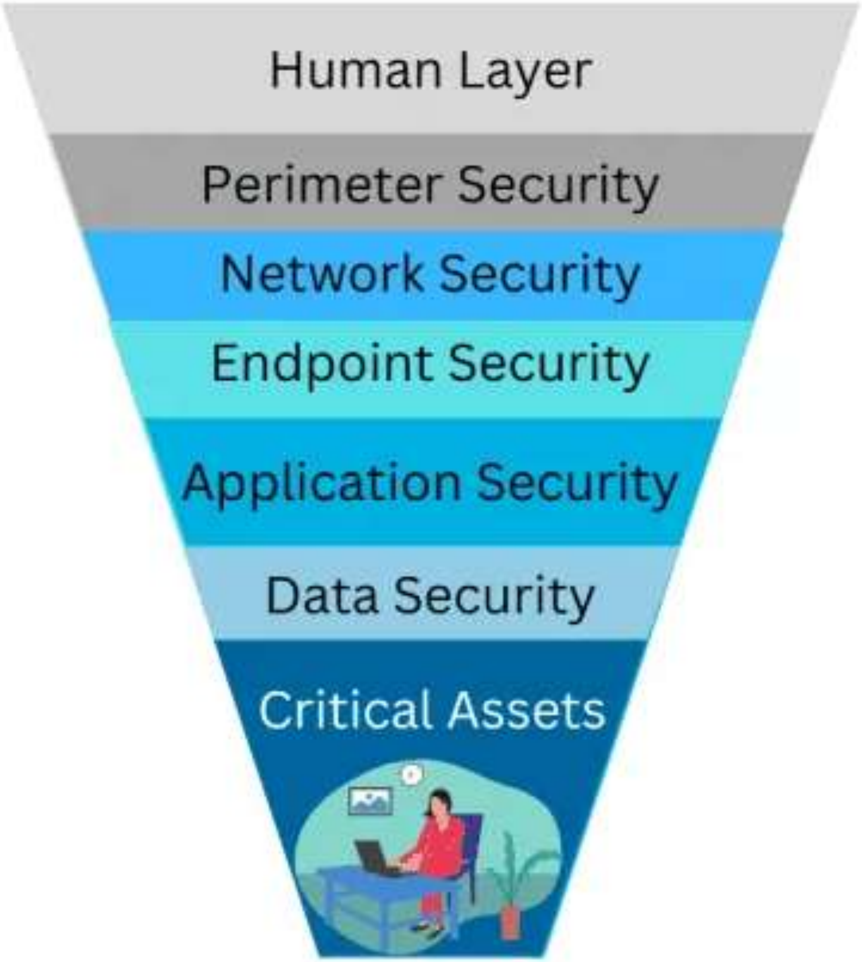


Bond Funding

HVS
HURON VALLEY SCHOOLS

Barton Malow

Cybersecurity Attack Vectors



Teamwork	Security is not just an IT venture. It takes the entire organization
The Human Factor	The biggest vulnerability for every org is people
Physical	Operations departments are vital to the physical security plan
Tech	Technology infrastructure is vulnerable to ransomware and other attacks

Tabletop: Scenario

Incident Response Plan

Sample Plan

CISA

Tabletop Handbook

Following the most recent pay date, a report from Human Resources indicates that 8 employees did not receive their paychecks, despite having up-to-date account information and enabling direct deposit for their accounts.

IT staff receive an unusually high number of reports from faculty and staff who are unable to access their employee accounts. Staff members are seeing error messages that their credentials are invalid, or their account no longer exists in the system.

Faculty and staff who are still logged are presented with the following message on their devices: "We own your data. For $250,000 in Bitcoin, your files will be returned. Submit payment to the wallet below within 72 hours, or everything will be posted for sale on the dark web."

Discussion Questions

- You are in a war room to handle this, who else is there?
- Technology Resources will be down for days, what is your plan?
- Based on these events, what are your priorities?
- How long can you maintain alternative procedures for student instruction?
- Who would you call first? Second?
- How will you handle the press?
- What actions would be taken based on your incident response plan?
- Does your organization have an incident response plan?
- What is the decision-making process for ransomware payment?
- How are your cyber insurance providers involved in your procedures?
- What are the advantages/disadvantages of agreeing/refusing to pay?
- What is your threshold for contacting law enforcement during a cyber incident?

CISA: Cybersecurity & Infrastructure Security Agency

To reduce your risk of successful ransomware attack (https://www.cisa.gov/stopransomware):

- Use multi-factor authentication for any external access to your systems.
- Always run up-to-date software (patch, patch, patch).
- Have good offline backups.
- Develop and practice your incident response plan.
- Use CISA's free Cyber Hygiene scans to help you understand and manage external vulnerabilities (things that the bad guys can see from outside your network).

https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services

Kelley Goldblatt/ CISA
Contact: Kelley.Goldblatt@hq.dhs.gov / 202-893-2304

Cybersecurity Planning Tips

Involve all Stakeholders
Build awareness with all staff, management and IT all on the same page

Review the Plan Often
The threat landscape is always changing. Review and update your plan regularly

Get Professional Help

Use help from a professional cybersecurity firm when needed

Cybersecurity Audit

Self Access

MISecure Quick Self Audit
https://misecure.org/selfauditdct/

Get Help

Consider hiring a vendor to conduct an Independent Cybersecurity Assessment using the CIS Controls

Use MIDEAL

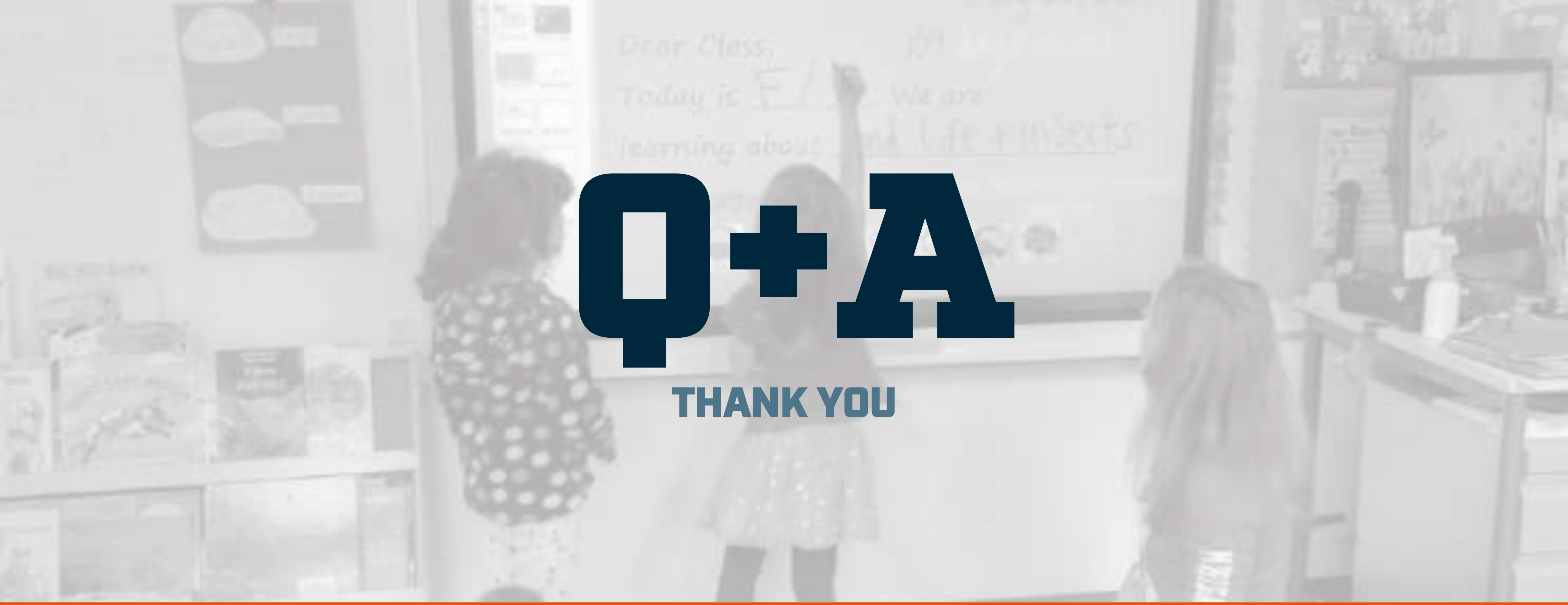
Contracts are available on Michigan's MIDEAL si third party cyber assessment by hiring one of the pre-approved vendors for Local Public Entities in Michigan: https://www.michigan.gov/cyberpartners and click on MIDEAL Assessments.

Cybersecurity Pillars

- **Identifying assets.** The first step in any cybersecurity plan is to identify all of the assets that need to be protected. This includes both physical assets, such as computers and servers, and digital assets, such as data and intellectual property.
- **Protecting assets.** Once you know what assets need to be protected, you need to put in place measures to protect them. This may include implementing security controls, such as firewalls and intrusion detection systems, and training employees on security best practices.
- **Detecting threats.** No security system is perfect, so it's important to have measures in place to detect threats. This may include monitoring network traffic for suspicious activity and using threat intelligence to identify potential attacks.
- **Responding to threats.** If a threat is detected, you need to have a plan in place to respond to it. This may involve isolating the affected systems, restoring data from backups, and notifying law enforcement.
- **Recovering from incidents.** Even if you have a good plan in place, there's always the possibility that a security incident will occur. It's important to have a plan in place for recovering from these incidents. This may involve restoring data from backups, rebuilding systems, and notifying customers and partners.

Framework

CIS Controls



Q+A

THANK YOU

HURON VALLEY SCHOOLS

Barton Malow