VERMONT
AGENCY OF EDUCATION

1 National Life Drive, Davis 5, Montpelier, VT 05620-2501
(p) 802-828-1130 | (f) 802-828-6430 | education.vermont.gov

School Cybersecurity

Purpose

This advisory is intended to provide Vermont supervisory unions and school districts with information and resources as a guide to address cybersecurity and initiate planning activities to guard against cyberattacks.

Overview

Cybersecurity refers to the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. [1]

Concern regarding cyberattacks on school network systems continues to grow. The U.S. Cybersecurity and Infrastructure Agency (CISA) recently reported the following: "Numerous reports of cyberattacks against K-12 educational institutions continue to be reported to CISA, FBI and the Multi-State Information Sharing and Analysis Center (MS-ISAC). According to MS-ISAC data, the percentage of reported ransomware incidents against K-12 schools increased at the beginning of the 2020 school year. In August and September, 57 percent of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28 percent of all reported ransomware incidents from January through July." [2]

Vermont SU/SD share this concern. The pandemic forced schools to rely heavily on their networks to provide accessibility to students, teachers, and staff to enable daily work to continue as systems had to move flexibly between remote, hybrid and in-person learning. This change has prompted many districts to assess vulnerabilities in their networks that could be exploited by nefarious individuals. Establishing a cybersecurity framework for a district will help schools better manage and reduce their cybersecurity risk.

Risk can come from both external and internal players. The U.S. Department of Education's Privacy Technical Assistance Program describes the threat. "Although electronic attacks by hackers and other cyber-criminals are a common cause of data breaches, other types of breaches occur regularly as well. 'Insider threats,' or threats coming from inside the organization, are also common and often involve employees accidentally, unknowingly, or maliciously mishandling, exposing, or losing sensitive data." [3] School districts that establish cybersecurity policies and procedures, that are understood and practiced by their education communities, create a significant deterrent to successful cyberattacks.

Contact Information:

If you have questions about this document or would like additional information, please contact:

Lisa Helme, Student Pathways Division at lisa.helme@vermont.gov or (802) 828-6956.

Roles and Responsibilities

As SU/SD approach planning activities, it is important to remember that cybersecurity is not just the responsibility of the information technology staff. "In this era of persistent cyber threats, an organization can be secure only with the active participation of everyone. Unfortunately, many organizations limit security responsibilities to designated security personnel that perform specialized security functions. Effective security must be enterprise-wide, involving everyone in fulfilling security responsibilities. Each member of the group, from the newest employee to the chief executive, holds the power to harm or to help, to weaken or strengthen, the organization's security posture." [4]

As you examine the cybersecurity framework in this document you will note that the internal review covers a wide range of stakeholders within the district and school. Stakeholders include *everyone* who utilizes the network that connects educational, financial, operational, and personal functions. AOE recommends districts and schools conducting cybersecurity planning mindfully include representatives from throughout the educational community to build a cyber-aware and resilient culture.

Cybersecurity Frameworks

National resources and organizations exist to guide districts in their cyber planning. Key among those organizations is the National Institute of Standards and Technology (NIST). NIST is a federal agency within the United States Department of Commerce. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST also is responsible for establishing computer and information technology-related standards and guidelines for federal agencies to use.

In 2014, NIST released a Cybersecurity Framework (CSF). In 2018, a major update to the CSF was completed. NIST continually works to keep these standards updated. The goal of the CSF is to create a common language, set of standards, and easily executable series of goals for improving cybersecurity and limiting cybersecurity risk. These standards are completely optional and are not required by any business or organization operating outside of the federal government. By Presidential Executive Order, in 2017 CSF was named as the standard to which all government information technology is held.

Vermont SU/SD can benefit from reviewing the NIST CSF and assessing their district's current cybersecurity plans. NIST offers a comprehensive and technical review of the CSF on their website. However, this advisory will focus just on NIST-proposed starting activities that can enable a district to implement a complete cybersecurity plan. For further assistance, please see the AOE companion document, Cybersecurity Breach Planning Rubric.

The CSF is organized by five key functions. The activities invite a district to examine their cybersecurity risk management and related communications among both internal and external stakeholders. Function identifiers (i.e. district instead of enterprise) were changed to best reflect the perspective of education stakeholders. The complete document is found in the NIST quick start guide. All material is used with permission courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce.

Identify

DEVELOP AN ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK TO SYSTEMS, ASSETS, DATA AND CAPABILITIES

- **Identify critical enterprise processes and assets:** What are your district's activities that absolutely must continue in order to be viable?
- **Document information flows:** What type of information does your district collect and use and where is it located and accessed by stakeholders?
- **Maintain hardware and software inventory:** Have an understanding of the computers and software in your district because they are frequently entry points for malicious actors. The inventory can be as simple as a spreadsheet.
- **Establish policies for cybersecurity that include roles and responsibilities:** These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems and support critical enterprise processes.
- **Identify threats, vulnerabilities, and risk to assets:** Ensure risk management processes are established and managed to ensure internal and external threats are identified, assessed, and documented in risk registers. Risk responses should be identified and prioritized, executed, and results monitored.

Protect

DEVELOP AND IMPLEMENT THE APPROPRIATE SAFEGUARDS TO ENSURE DELIVERY OF SERVICES

- **Manage access to assets and information:** Create unique accounts for each employee and ensure each user only has access to the applications and computers needed for their jobs. Authenticate users and manage physical access to devices.
- **Protect sensitive data:** Make sure sensitive data is protected by encryption and securely delete/destroy data when it is no longer needed.
- **Conduct regular backups:** Many operating systems have built-in backup capabilities. A good practice is to keep one frequently backed up set of data offline to protect against ransomware.
- **Protect your devices:** Consider installing host-based firewalls, apply uniform configurations to devices and control changes, disable device services not needed to support mission functions, and have a policy in-place that devices are disposed of securely.

- **Manage device vulnerabilities:** Regularly update operation systems and applications installed on computers and other devices to protect them from attack.
- **Train users:** Regularly train and retrain all users on cybersecurity policies and procedures.

Detect

DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO IDENTIFY THE OCCURRENCE OF A CYBERSECURITY EVENT

- **Test and update detection processes:** Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity.
- **Know the expected data flows for your enterprise:** If you know what and how data is expected to flow through you district or school, you are much more likely to notice when the unexpected happens—never a good thing when it comes to cybersecurity.
- **Maintain and monitor logs:** Logs record events such as changes to systems or accounts as well as the initiation of communication channels. Logs are crucial to identify anomalies in your district or school computers and applications.
- **Understand the impact of cybersecurity events:** If a cybersecurity event is detected, work quickly and thoroughly to understand the breadth and depth of the impact. Seek help. Communicate information on the event with the appropriate stakeholders.

Respond

DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO TAKE ACTION REGARDING A DETECTED CYBERSECURITY EVENT

- **Ensure response plans are tested:** Test response plans to make sure each person knows their responsibilities in executing the plan. This includes knowing any legal reporting requirements or required information sharing.
- **Ensure response plans are updated:** Testing the plan will reveal needed improvements. Update your plan with lessons learned.
- **Coordinate with internal and eternal stakeholders:** Make sure your response plans and updates include all key stakeholders and external service providers. They can contribute to improvements in planning and execution.

Recover

DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO MAINTAIN PLANS FOR RESILIENCE AND TO RESTORE CAPABILITIES IMPAIRED DUE TO A CYBERSECURITY EVENT

- **Communicate with internal and external stakeholders:** Part of recovery depends upon effective communication. Recovery plans should account for what, how, and when information will be shared with various stakeholders so all interested parties receive the information they need but no inappropriate information is shared.
- **Ensure recovery plan are updated:** As with response plans, update recovery plans with lessons learned.
- **Manage public relations and organization reputation:** When developing a recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely – not reactionary.

Cybersecurity is everyone's concern within the district and school community. Collaborative planning will promote an understanding of the strengths, weaknesses, and opportunities present within your existing cybersecurity posture. As noted earlier in this document, AOE has composed a Cybersecurity Breach Planning Rubric from NIST and US DOE resources to aid districts and schools in evaluating their cyber-readiness.

Resources

Below is a list of organizations and resources on cybersecurity.

Council for School Networking (CoSN): CoSN is a professional association for school system technology leaders. CoSN offers a cybersecurity toolkit to help schools assess their risk and a planning rubric to provide guidance in school planning efforts.

Cybersecurity & Infrastructure Security Agency (CISA): CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. CISA has a page of free cybersecurity services and tools.

Multi State Information Sharing and Analysis Center (MS-ISAC): The mission of the MS- ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. Membership is free to school districts. MS-ISAC offers network vulnerability assessments, cyberthreat alerts and other related services. As of March, 2022, 24 Vermont school districts were members. Free Tabletop Exercises.

National Cybersecurity Center of Excellence (NCCoE): The center is part of the Applied Cybersecurity Division of NIST's Information Technology Laboratory. NCCoE brings together private industry, government agencies, and academia to create practical, standards-based solution. The center website features a security guidance section with information based on specific technology, sector, and status use.

National Institute of Science and Technology (NIST): NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, April 25, 2019. Other resources include NIST publications. "Zero Trust Architecture."

SchoolSafety.gov: U.S. government collaborative of federal school safety resources, including cybersecurity resources.

U.S. Department of Education (US DOE): The department administers and enforces student privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). In addition, the US DOE provides technical assistance to help schools and school districts safeguard information about students through the Privacy Technical Assistance Center.

NIST Cybersecurity Framework

---

[1] National Institute of Standards and Technology (NIST), Computer Security Resource Center, https://csrc.nist.gov/glossary/term/cybersecurity

[2] Cybersecurity and Infrastructure Security Agency, "Back to School Campaign," August 9, 2021. https://www.cisa.gov/blog/2021/08/09/back-school-campaign

[3] Privacy Technical Assistance Center, US Department of Education, "Data Breach Response Checklist." https://studentprivacy.ed.gov/resources/data-breach-response-checklist

[4] National Initiative for Cybersecurity Education Working Group, National Institute of Standards and Technology, "Cybersecurity is Everyone's Job." https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf