LEADING EDUCATION INNOVATION

A Members-Only Report

What School Leaders Need to Know About the Internet of Things

IoT devices offer many opportunities to automate processes within a school system; however, they are not a neutral addition to the organization's technology toolkit. Like other technologies, implementing IoT devices in the district requires careful review and planning to ensure security is correctly architected and in place before implementation, and to implement a plan for supporting and sustaining the IoT devices once implemented.

What School Leaders Need To Know About the Internet of Things

Overview: What is the Internet of Things (IoT)?

The Internet of Things, or IoT as it is commonly known, encompasses a wide range of devices that have built in sensors, computer processing, software, and network (wireless or wired) technologies that collect and exchange data over the Internet or other communication networks. These devices are already widely deployed in school systems today and include, but are not limited to:

- Building Automation and Management Systems - Utility Management: HVAC systems, including thermostats
- Classroom technologies: greenhouses, beehives, lighting, science and CTE program equipment, automotive, nursing, fire, etc.
- Communications devices: Speakers, bells, digital signage, and intercom systems
- Environmental: moisture, mold, temperature fluctuations
- Food services: Coffee pots, vending machines, refrigerators
- Lighting: Smart light bulbs, window shades, temperature and natural light management systems,
- Robots: floor cleaning systems, food delivery systems, etc.
- Security systems: security cameras, door locks, perimeter security, key cards, vape sensors, transportation systems

Each of these devices collects and processes data, transfers information and performs a function within the school environment. Often these devices are overlooked or not recognized as the network attached computing devices they are. Identifying what systems are already in place that can help districts develop a plan to monitor and manage IoT devices before further expanding the technical footprint.

IoT Opportunities

The utilization of IoT devices represents opportunities for school systems to automate many manual processes, e.g. cleaning, environmental management (lights, heat, cooling), food management, security, etc. and reduce costs in non-technology areas. The opportunities these implementations bring should be evaluated in balance with security implications, the information technology management and support needed to securely manage and operate the devices and the total cost of ownership to the organization.

Security Implications

The deployment of IoT devices in school systems has an abundance of security implications for the organization. IoT devices can quickly become risks to the institution's network. There are already examples of organizations being hacked through HVAC systems, smart energy systems and other IoT solutions. The following questions should be addressed for each IoT implementation:

- What data is being collected by the device, where is it stored and who has access to it? Who owns the data collected from each device? What are the protections for any personally identifiable data?
- Does the device require remote access by vendors? How is access managed and limited only to the approved devices for each vendor?
- How will the organization schedule and manage each device's firmware and operating system updates?
- Have the factory default passwords been changed? How will the organization create and manage service accounts necessary to manage the devices?

Managing IoT

Internet of Things devices are not "set and forget" devices. Like any other computing device, they require management and oversight. Here are eight steps every school system should follow to manage the influx of IoT devices into the organization.

1. Inventory management - establish a process for identifying and inventorying IoT devices so the school system knows what devices are already in place. An accurate inventory is essential to conduct before you start adding additional devices to your environment. Include an existing infrastructure survey: electricity, plumbing, internet cabling/switching, sewer, etc.

2. Identify the problem the school system is trying to solve and the intended use of the IoT device before purchasing a solution. Purposes may include savings, operational efficiency, security, etc.

3. Complete a total cost of ownership (TCO) evaluation that determines what the cost and impact, beyond just the equipment, is to the school system of implementing the IoT solution. For example, a TCO evaluation may determine that the cost of smart lighting systems, including the management of those systems, is off-set within two years of installation and may also identify that the savings in electricity for the school system may result in an unanticipated fine for using too-little electricity.

4. Pre-purchase technology and security evaluation - establish a process by which all school system personnel must collaborate with the CTO/IT director before purchasing any devices that are "WiFi," "Smart," or "Network attached." Devices that plug into or connect wirelessly to the school system network represent a risk to the organization's whole infrastructure. This review process should include a determination by the CTO/IT director that the device meets the following requirements:
    a. **Enterprise grade IoT, not consumer grade (home devices)**. Enterprise IoT solutions are designed to run on organizational networks and generally

have better security controls than the equivalent home devices. Many home use devices are not designed to secure student and staff information privacy.

b. Systems are maintained and upgraded on a regular schedule by the vendor and can be managed in accordance with the organization's security policies
c. CIO/CTO and school system staff review products with peers and identify known concerns or issues before devices are purchased.
d. Assess if the solution is scalable and integrates into the existing technology environment.

5. Pre-purchase data privacy review. The product and contract should be reviewed to determine if it meets the school system's requirements. The contract should clearly specify who owns the data, if any data is covered by privacy considerations, and how that data is handled or used by the vendor or the school system.

6. Implementation process. The technology team should be involved with the implementation of each IoT solution and evaluate where devices go on the network, how network segmentation and isolation can support secure deployment, and

7. Plan for remote access. Who has remote access to IoT devices? What security is in place to protect IoT devices from being inappropriately accessed, and how to ensure the right people inside and outside your organization have access? It is unlikely you will be able to eliminate the need for remote access, so instead it is important to have clear processes and procedures for how IoT devices will be accessed and managed remotely, and how vendors will request access to conduct work on these devices on behalf of the school system.

8. Ongoing support, maintenance and monitoring. Once an IoT solution is in place, it should be transitioned into maintenance mode. Responsibility for maintaining the firmware and operating system should be clearly defined, documented and scheduled. If not directly responsible for maintenance, the school system IT team

should identify a process for monitoring the devices and ensuring they are managed and maintained in accordance with school system procedures and the contract.

Conclusion

IoT devices offer many opportunities to automate processes within a school system; however, they are not a neutral addition to the organization's technology toolkit. Like other technologies, implementing IoT devices in the district requires careful review and planning to ensure security is correctly architected and in place before implementation, and to implement a plan for supporting and sustaining the IoT devices once implemented.

About CoSN:
CoSN, the national association of school system technology leaders, believes that technology is an essential component of learning today, and is deeply committed to the use and distribution of technology in school systems. However, all technologies must be properly assessed for design and appropriateness in the modern classroom. Educators and companies alike must recognize and uphold their responsibilities to protect the privacy of student data.

Working together, educators and the private sector serve millions of students by providing them with the rich digital learning experiences and access needed to succeed in college, work and life. That partnership is critical to ensuring that students will have the tools necessary for success in the 21st century.

Special thanks to CoSN's Networking & Systems Design Advisory, lead by project Director Amy McLaughlin, CETL

Consortium for School Networking 1325 G St, NW, Suite 420, Washington, DC 20005