The Impact of Cyber-Physical Security Systems on IT Infrastructure

KEEPING YOUR NETWORK ROBUST AND SECURE

A CoSN Member Resource
October 2018

Cyber-Physical Security System (CPSS) management requires close coordination between the district leadership, facilities personnel, and IT staff. The interaction of physical and cyber systems can add significant complexity to school security planning. These hybrid systems can have significant impacts on network infrastructure, IT security, data privacy, budgeting, and staffing. To ensure that school networks are adequately prepared to handle CPSS, consider the following areas of potential impact:

Network Bandwith

CPSS can have a significant impact on network bandwidth. Streaming video, for example, is a high bandwidth application that can negatively impact network performance. Consider installing modern cameras with improved compression algorithms to mitigate bandwidth demand. Local storage and/or limiting real-time recording to activity triggers, such as motion detection or a door opening, can also reduce network impacts. Implementing Quality of Service (QoS) to **prioritize network traffic** can mitigate the impact of CPSS traffic on school networks and allow it to be prioritized during a security event. Employ **network segregation** by putting cyber-physical security devices such as door monitors and video cameras on separate physical or virtual networks. This can protect the main network from exposure in the event of a security incident involving the CPSS.

Device Security

Before implementing CPSS, determine how product vendors guard against unauthorized device access. Proactively monitor equipment for potential breaches; consider utilizing internal firewalls, micro-segmented networks, and/or a port based security authentication standard such as IEEE 802.1x to protect the devices. CPSS devices should be managed as part of a larger **Identity and Access Management (IAM)** process. Implement role-based control and limit CPSS administrative access to trained and trusted IT/security personnel. At a minimum, change the default password of all CPSS equipment to a strong passphrase using industry standards such as those outlined in the NIST Digital Identity Guidelines. Consider implementing systems that support multiple users, multi-factor authentication, and integration with other identity management systems. If CPSS equipment has a management console, ensure it is using **https**. Keep device **updates and patches** current to minimize the risk posed by software vulnerabilities. Determine how CPSS access will **logged, audited and monitored**; review system logs regularly to ensure systems have not been compromised. Develop clear documentation, policies and procedures around **Third-Party Access** to CPSS devices and require a VPN connection for external access.

Data Management

Understand how CPSS data will be protected, stored, and archived. Determine if data will be stored locally, at a central district location, or with a third-party vendor. Some data collection systems support forensic capabilities that maintain the chain of custody, including the control, transfer, analysis, and disposition of physical or electronic evidence. Become familiar with all state or district **data archiving** requirements and plan carefully to ensure adequate data storage space for CPSS data. Consider **data interoperability** when evaluating CPSS; the ease with which data can be transferred between other systems, such as student information systems or HR software, can significantly impact implementation costs and staff time.

Biometric Data

Before implementing biometric data systems such as facial recognition or fingerprint recognition, consider whether the data will be stored locally or remotely and evaluate the security measures in place. If using third party storage, read the vendor's terms of service and privacy policies carefully to ensure they meet the requirements of state and federal law. Consider whether the security risks of a potential breach outweigh the potential benefits of CPSS technology. See CoSN's Protecting Privacy in Connected Learning toolkit for valuable information about managing student data privacy. The U.S. Department of Education's Privacy Technical Assistance Center is also an excellent resource.

Facilities

The installation of CPSS equipment may impact facility power, cooling, staffing and physical security. Some considerations include:

- **Power.** Find out how long CPSS equipment needs to be kept running in case of a power failure. Identify power or backup solutions that meet these requirements and the costs of sustaining and maintaining them. Determine if the network has adequate port capacity and power to support Power over Ethernet; some new devices, such as smart lighting, may exceed existing capacity. For additional information see the IEEE standards for Power over Ethernet, Power over Ethernet+, and Power over Ethernet++.
- **Cooling.** Evaluate the impact of CPSS on existing cooling systems and determine if additional cooling/power capacity is needed.
- **Staffing.** Identify who will provide technical support for CPSS systems and interface with the vendor support when necessary. Ensure that adequately trained personnel are available to manage both the front and back end of CPSS.
- **Physical Security.** Keep CPSS equipment physically secured behind locked doors or cabinets and carefully manage cabling to prevent the physical hacking or disabling of the CPSS network.

CoSN is grateful to the following sponsors for their support of the Cybersecurity Initiative:
CDW G . Cisco . ENA . Fortinet . iboss . Microsoft