Guidepost

EDUCATION SECTOR COMMUNICATION CONSIDERATIONS AND NETWORK IMPLICATIONS BROUGHT TO LIGHT BY COVID

The pandemic has thrown school districts and community colleges quite a few curve balls including, at times, seeing their campuses devoid of students and regular day-to-day activity. During this time, we've seen our education clients adjust the focus of their security and safety programs and place renewed emphasis on improving mass notifications capabilities. It has been particularly interesting, and to some degree surprising, to see the number of educational institutions that operate with non-functional mass notification equipment, network-based equipment with no emergency back-up, old telephone systems, and in some cases no mass notification capabilities at all.

Fundamental to effective mass notification is the ability to communicate across all communication channels with the intent to keep people safe, informed and engaged. This requires the ability to send and receive intelligible messaging whether it be to an individual, group, or larger audience — for example an entire school campus. In carrying out scores of school security assessments, we've identified well-intentioned communication systems and device installations that have lacked wider operational considerations and needs, such as interfaced platforms, multiple systems accessibility to make calls, restricted permissions, untested equipment, incorrect programming of network residing devices and cyber vulnerabilities due to factory settings not being re-programmed. All these shortcomings sound problematic, and they are, but all can be fixed. This is where a technology solutions consultant can help by providing guidance and strategies to ensure that any new system or component is operationally correct, supports other technologies in use, is scalable, sustainable, and hardened against cyber threats.

The continued adoption by many education institutions to implement internet protocol (IP) power-over-ethernet (PoE) mass communications addressable devices onto local and wide area networks is now commonplace, and with it is the need to maintain secure networks mitigating opportunities for hackers to infiltrate potential vulnerabilities. In our

experience we have observed critical weaknesses in network management from simple lack of network protection, hardening and monitoring of activity to fundamental issues such as lack of financing and resources to successfully manage the ever-expanding dependency of IT networks to support critical security and communications systems.

A Focus on Network Security

An operations-centric approach to applying technology to enhance safety and security rather than drive operations ensures that the unseen backbone remains solid and receives a continual health-check to mitigate unseen threats.

A cybersecurity performance and vulnerability tool, like the industry-leading GearBox, can be used as a "push and go" device to perform a comprehensive network device vulnerability analysis. The GearBox tool finds, assesses, and reports security and performance vulnerabilities of Internet-of-Things (IoT) network devices simply by connecting to the network and performing a comprehensive scan. This is a simple, but hugely effective step in maintaining secure networks by ensuring that known vulnerabilities (such as confirming that all network device factory settings passwords have been changed by the systems installation contractor upon installation) are not exploited by entities seeking to cause harm your network. Moreover, scanning with a tool like GearBox is a critical step in helping to maintain a secure cybersecurity posture that mitigates threats and vulnerabilities as a standard systems commissioning practice. The GearBox can be used to support any network systems installation, including mass notification, video surveillance, access control and others.

Reviewing and confirming any vulnerabilities created during the installation of new network devices should be a final systems testing norm and can help determine the success of the installation. An independent third-party consultant can bring an objective viewpoint to the process ensuring all measures maintain both physical and cybersecurity postures are addressed.

NICK HEYWOOD PMP

Associate Vice President

Nick Heywood is an experienced security consultant and project manager who excels at performing security and safety assessments and developing existing conditions observations into workable solutions that enhance a facility's security posture. Mr. Heywood has overseen projects in verticals including healthcare, corporate, detention and education.