Education and medical campuses are complex 24 x 7 multibuilding environments that must be secured to protect the physical and digital safety of patients, students, and family members as well as visitors and staff.

Securing Smart Campuses: Do You Know the Risks?

October 2019

Questions posed by: Fortinet
Answers by: Lynne A. Dunbrack, Group Vice President

Q. Why should educational and medical campuses pursue a "security first" strategy when it comes to deploying smart campus technology?

A. Smart buildings found on educational and medical campuses (often referred to as smart campuses) represent the convergence of operational technology (OT) and information technology (IT). Building management (or automation) systems are increasingly being connected to the internet, providing a broader attack surface for bad actors to exploit smart building technology, such as connected heating, ventilating, and air-conditioning (HVAC) systems, to gain unauthorized access to IT systems and valuable data stores. Thus, campuses' smart building technologies present a new attack vector that enterprises need to secure to protect IT assets and operational building functions.

Schools and healthcare organizations must take a "security first" stance to counter the often dismal security posture of smart building solutions that do not have security built in from the ground up. It is not uncommon for older building automation/management systems and industrial controls to have minimal password protection. Embedded operating systems are not adequately patched to the latest security upgrades and, in some cases, are no longer supported by the manufacturer. Connected smart building technologies and devices from multiple vendors only compound security challenges facing smart campuses today.

Q. What are the top 3 considerations for IT security professionals when investing in smart campus technology to deliver a secure environment?

A. First and foremost, IT security professionals should develop a comprehensive plan to inventory the smart building technologies, including devices and sensors, across the campus; conduct a thorough risk assessment to identify and prioritize potential security vulnerabilities; and develop a plan and a budget for remediation. Adequate time should be allocated given the dozens of point solutions from as many vendors, plus the hundreds to thousands of devices and sensors deployed across the campus that:

» Improve the occupants' experience: Air quality monitoring, smart HVAC, smart kiosks, smart parking, wayfinding
» **Make operations more efficient:** Real-time location services, smart elevators, predictive maintenance

» **Protect buildings and occupants:** Building access control, large-scale emergency response systems, physical security and cybersecurity, and video surveillance

» **Enhance sustainability:** Smart meters, smart HVAC, smart lighting/sensors

Alongside the inventory of smart building technologies, a risk assessment should be completed to identify potential security vulnerabilities. What is the security update status for each application and its associated devices? Is the operating system still supported, or has it been sunsetted? Are there any known zero-day vulnerabilities? How strong are the passwords for the systems? What level of integration exists between the smart building solutions and other OT/IT systems? In other words, if a smart building technology was breached, how easy would it be for a cybercriminal to traverse the network to access more valuable IT assets such as student, patient, or employee financial information or protected health information of patients or students? Once IT security professionals understand the magnitude of the security risks, then they should develop a plan that prioritizes and appropriately funds the remediation effort to mitigate the risk of a security breach via smart building technologies.

Q. Ensuring the physical and digital safety of patients and students is essential today. What key technologies are smart campuses deploying to protect patients, students, family members, staff, and visitors?

A. Sadly, workplace violence is on the rise across schools and healthcare organizations. Schools need to protect their students and educators against general crime and, in extreme cases, active shooters. Emergency rooms and inpatient psychiatric units are common settings for workplace violence perpetrated by patients against healthcare providers. Not surprisingly, these patients tend to exhibit altered mental status associated with dementia, delirium, substance intoxication, or decompensated mental illness. Patients in police custody because of gang activity or other street violence are also more likely to be violent and/or have violent visitors.*

Physical security and cybersecurity are becoming intertwined as more physical security devices, such as video surveillance, employee badges, and building access controls, are being connected to the network and stream data to be aggregated, analyzed, and monitored as part of the greater Internet of Things (IoT) initiative. Embedded artificial intelligence can provide insights to detect anomalies in behavior or appearances. Activity logs generated by employee badges and building access controls identify employees accessing buildings at unusual hours or attempting to access unauthorized areas. Gun detection capabilities as part of video surveillance enable campus law enforcement officers to respond proactively to potentially dangerous activity. As a result of this growing convergence between physical security and cybersecurity, ownership of and responsibility for networked physical devices are shifting from facility operations to the IT.

For example, 22% of providers responding to IDC’s 2018 *U.S. Healthcare Provider Technology and Services Survey* reported that physical security measures were a top area for increased IT services spend.

Q. What is the potential impact a security incident could have on a smart campus?

A. Healthcare organizations and schools must comply with industry privacy and security regulations that protect personally identifiable and sensitive information about patients and students — the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), respectively. Both regulations have stringent provisions for granting who has access to protected information and for what purposes, the authorized sharing of student or patient information, and how long data must be retained. Failure to comply with these regulations has serious consequences: Schools could lose federal funding, and healthcare organizations could face significant financial penalties.

More insidious than privacy breaches involving unauthorized data disclosures or human errors are cyberattacks involving malware and ransomware. While schools and healthcare organizations are increasing their security spend to protect against such attacks, cybercriminals know that these systems are vulnerable and easy to exploit given historical low levels of IT funding overall and lack of strong security in particular. Across the United States, smart campuses have had to cancel school or clinical procedures after their IT systems were taken hostage until a ransom was paid or IT was able recover from a backup of impacted systems. For healthcare organizations, this not only puts patient safety at risk but also threatens the financial health of the institution if patients have to be diverted to a competitor to receive emergency care.

Q. What security recommendations do you have for healthcare and educational organizations as they deploy smart campus solutions?

A. Smart campuses are connected assets with hundreds to thousands of sensors and devices at the edge that are difficult to secure and thus create a broad attack surface. The threat landscape is rapidly changing, making the increased risk of an attack inevitable. It’s only a matter of when, not if, cybercriminals will attack smart campuses. While high-profile cyberattacks make headline news, not all threats originate from nation-states or organized crime. Schools and healthcare organizations are also at risk for domestic and on-premise attacks. They must change their approaches to cybersecurity to keep pace and adequately protect themselves against cyberattacks that result in financial, operational, technical, and reputational damages.

A "security first" approach is essential. Smart campus IT security professionals must think about security and compliance in terms of business risk to providing ongoing educational and clinical services. IDC recommends the following security best practices for smart campuses:

» Develop an overarching security plan that includes smart building technology. Too often smart building technology and its associated security vulnerabilities are overlooked by IT security professionals because these systems were acquired and maintained by a separate department or business unit. However, smart building technologies have been exploited to gain access to the enterprise network and IT systems.

» Involve key stakeholders early in the process across the enterprise. The convergence of physical security and cybersecurity will compel multidisciplinary teams to work together to leverage security technology to secure the physical and digital safety of students, patients, family members, staff, and visitors.
» **Increase visibility of smart building devices at the edge and on the network.** The proliferation of sensors and devices is creating an essentially borderless attack surface that is growing exponentially, thus putting smart campuses at greater risk for a privacy or security breach. Any device that is connected to the network or can be accessed remotely should be evaluated for its potential to be exploited by cybercriminals.

» **Deploy internal segmentation firewalls (ISFWs) to provide an additional layer of protection.** Segmenting the network with strategically placed ISFWs in front of vulnerable IT assets prevents unfettered access to the network if smart building technologies are used as a vector for a cyberattack.

» **Deploy on a platform solution/fabric.** Bridging the divide between digital and physical security requires a holistic platform approach using security fabric to provide an integrated view into security across the enterprise, avoiding siloed point solutions. Security fabric provides greater levels of integration and intelligence sharing between security products. Greater visibility into the network from a single pane of glass accelerates response and remediation in the event of a known or suspected attack.

» **Form a strategic relationship with your security technology supplier.** Smart campuses are inherently complex environments running 24 x 7 mission-critical applications. A true strategic partner understands your mission and will develop a security road map that will help you provide a secure and safe smart campus environment.

### About the Analyst

**Lynne A. Dunbrack, Group Vice President**

Lynne A. Dunbrack is Group Vice President for Public Sector, which includes IDC Government Insights and IDC Health Insights. She is a nationally recognized thought leader in the application of information technology to the business problems of the health industry. Her understanding of the needs of the health industry is grounded in experience over the past 35-plus years working as a consultant and in the field.
MESSAGE FROM THE SPONSOR

Fortinet is a worldwide provider of network security appliances and a market leader in network security. Our products and subscription services provide broad, integrated, and high-performance protection against advanced threats while simplifying the IT security infrastructure. NASDAQ: FTNT. Learn more about Fortinet solutions at https://www.fortinet.com/solutions/