Healthcare Security and Environmental Design

By Steven Nibbelink, CHPA, CA-AM

Previously we have studied some of the more familiar regulatory agencies and standards that govern the safety and security aspects of the healthcare environment as well as operational security issues, such as workplace violence that hospitals, urgent care clinics and other providers face on a routine basis. Continuing our review of safety and security issues in the healthcare environment, this latest paper in our four-part series of healthcare security trends will focus on physical security and the importance of proper design and implementation of security technology when protecting such environments.

Physical Security

Let us pretend for a moment that we have traveled back to medieval times and that you are the ruler of a kingdom. You are in the process of constructing a new castle from which to govern your empire, but there are both internal and external threats that you must take into consideration. First, you do not want those that should not be in the castle to have free entry, so perhaps a moat or drawbridge is in order to allow only those that are authorized into the courtyard. A strong gate or portcullis would be used to deter resolute antagonists actively seeking entry to restricted areas. You would likely deploy a group of watchmen along an elevated parapet walk or on the tower to serve as lookouts should an intruder be sighted or a fire break out after hours inside the structure. And lastly you would need some type of notification device such as a bell or horn to be used to warn others that an incident was occurring and to raise a hue and cry so a timely response to the situation was forthcoming. While these archaic versions of access control, video surveillance and alarm systems worked for castles hundreds of years ago, their more modern equivalents still play a crucial role in the safety and security of any facility, particularly in the healthcare field.

Access Control

Appropriate access controls are a critical component to the security of any healthcare facility, regardless of the facility's size or complexity. Access control systems exist in many forms. For basic needs, there are master key systems that allow certain keys to open more locks than others based upon an employee's responsibilities, as well as keypad-style locks that require a code to open, allowing convenient access. For more secure areas, identification badge access systems and even biometric authentication technology such as iris, fingerprint or palm scanners may be used to restrict entry. One can also combine such systems to further increase security based upon need or circumstance, such as a high security area that requires two or more forms of authentication to access, such as a valid badge as well as the entry of a PIN code. Most methods of access control that use an authentication process rely upon one or more of these three attributes: something you have (a key or ID badge); something you know (a password or PIN code); and / or something you are (iris or fingerprint scan). Each of these attributes have their own strengths and weaknesses, but when designed properly, an access control system is a very effective means of increasing security.

Appropriate access controls are a critical component to the security of any healthcare facility, regardless of the facility's size or complexity.

In healthcare, there are numerous reasons that an effective and well-designed access control system should be foremost in any facility's security program. Healthcare facilities, from standalone clinics and urgent care centers all the way up to large acute care hospital campuses have patients, including children, that are at their most vulnerable. We must balance visitation of friends and family members with protection of these patients, but there are also a significant number of areas in which non-healthcare workers should not enter for their own safety (areas containing hazardous waste or other dangers, for example). Add to this that all healthcare facilities contain inherently valuable materials (such as controlled substances and protected health information) and the necessity for an effective access control system becomes very clear. Many regulatory agencies, such as the Joint Commission and the Urgent Care

Association of American already have specific standards requiring proof of limited access to security sensitive areas.[1,2] OSHA also gives specific recommendations regarding engineering and environmental controls as related to staff safety in OSHA #3148 "Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers."[3] While vital, a well-designed and properly implemented access control system is only one part of a holistic healthcare facility security program.

A well-designed and properly implemented access control system is only one part of a holistic healthcare facility security program.

Video Surveillance

Camera technology and the ability to take photographs and video recordings at any time and in almost any circumstance thanks to smart phones, tablets and associated apps have transformed our society. Once an expensive security component that required not only significant capital investment in hardware but also considerable time and labor to install and maintain, video surveillance systems of today have improved dramatically, delivering a range of benefits and a strong return on investment. Video surveillance now offers the ability to remotely view an area in real time and after an incident, helping with the reconstruction of an event or evidentiary purposes. And thanks to advances in hardware and software, cameras now can provide so much more. Gone are the days of a guard or operator sitting and watching a static screen, waiting for signs of suspicious activity (neither effective nor efficient). Today's cameras use motion detection algorithms to alert authorized users of any movement within the camera's field of view. They can also be programmed to detect activity based upon time of day, range of motion or even type of motion, such as someone leaving an unattended item in an area for a defined period of time. Another facet of video analytics includes license plate and facial recognition capabilities to determine the identity of a vehicle or a person. New advances in this field include cameras smart enough to even detect slips, trips and falls and send notifications immediately to authorized personnel.[4] All of this is in addition to the traditional role of crime prevention that video surveillance system provide.

Video surveillance now offers the ability to remotely view an area in real time and after an incident, helping with the reconstruction of an event or evidentiary purposes.

From vandalism to theft to more serious crimes such as robberies of pharmacies and urgent care clinics, video surveillance systems and their integrated analytics play a pivotal role in the deterrence and detection of many such activities and like access control systems, are prominently mentioned in many best practices and articles involving the securing of healthcare facilities.[5]

Alarms

One additional element in a well-designed physical security program for healthcare is that of alarm and notification systems. This category of security includes a broad spectrum of applications, including unauthorized entry / intrusion alarms, duress or panic alarms and integration with access control and video surveillance systems to create a multi-layered security solution. For example, an access controlled door sounds an alarm if forced or held open, and the closest camera automatically pans to view the location of the incident. Such integration was at one time prohibitively expensive for most companies, but with advances in communications and the convergence of functionality provided by modern security products, such systems are not only affordable but commonplace. While alarms detecting unauthorized entry are still the most common for many businesses, due to the increase in severity and frequency of workplace violence in the healthcare industry, many facilities and high-risk departments have adopted duress and panic alarms to summon assistance quickly when staff members are threatened. Like access control technology, panic buttons can take many forms, from the more traditional "fixed" panic button such as those installed under a desk to be activated discreetly if staff feel threatened, to a body-worn device that summons help and identifies the location of the staff member. Such personal panic devices are growing in popularity especially for those healthcare workers that deal with high-risk patient populations on a regular basis, such as emergency departments, urgent care centers and behavioral health units. There are now apps that can be installed on staff members' smartphones that provide similar functionality without the installation of expensive hardware and dedicated equipment.

A well-designed access control, video and alarm system can dramatically improve the current state of readiness and security posture of any healthcare facility.

A well-designed access control, video and alarm system can dramatically improve the current state of readiness and security posture of any healthcare facility. Such technology, in conjunction with appropriate training and processes for staff to follow can be a huge force multiplier in creating and maintaining a safe environment for themselves and their patients and can deliver operational benefits as well. When monitored by a professional alarm center, commonly known as a central station, services will include detailed reporting of alerts and access logs, the health of key systems, and customizable dashboards and notifications for your staff.

Network Security and the Internet of Things

Security and convenience are frequently at odds, especially in modern corporate networks that are challenged by trends like Bring Your Own Device (BYOD) and the "Internet of Things".
The Internet of Things, or IoT, is a term that refers to the connection of basically any device with an on/off switch or function to the internet[6]. From thermostats and fitness trackers to lighting and locks, the number of connected devices has grown dramatically in recent years, and the trend show no signs of slowing down. As a result, it has become very important to build an IoT strategy when designing and implementing a secure network. With so many devices running on the network, it's imperative that the proper tools and talent are leveraged to detect and defend against intrusions. Many erroneously think that they only need be concerned about unauthorized access to their computer or portable electronic devices like smartphones or tablets, but IoT devices introduce many other issues that have to be considered. Imagine a malicious actor hacking into IV infusion pumps to change their dosage settings, or disabling key building systems such as HVAC or lighting. This concern is so great that the U.S. has banned government use of certain telecommunications and surveillance products, citing "national security concerns."

Proper network design, along with ongoing monitoring and management can allow all the benefits of connected devices, while managing the risks.

Proper network design, along with ongoing monitoring and management can allow all the benefits of connected devices, while managing the risks. From determining bandwidth requirements and isolating sensitive network segments, to designing scalability for future business needs, effective planning and partnerships are critical for success.

In today's healthcare security environment, network security is a serious risk that, if not addressed, can result in data breaches, monetary fines to the organization and negative branding which is difficult to recover from.

Please join us for our final paper in the series in which we will explore cybersecurity issues and the growing importance for healthcare organizations of the safekeeping of their networks and protected information, as well as recent examples of why network security is one of the highest priorities for today's healthcare security practitioner.

Solutions for a safe, secure and welcoming environment

The "Reduction of Risk" is the same for Physical Security and Network Protection, you need all the elements of People, Process and Technology to be successful. In terms of physical security technology, what is best for your facility and operation – cloud-based solutions that leverage the internet and networking connectivity or premise-based solutions that are more traditional in structure and communications? Access Control, Video Surveillance and Alarm / Intrusion Technology all provide cloud-based applications to enhance your ability to perform the "command and control" function, utilizing the IT and networking world, to be able to observe and act on adverse events, from any location, at any time. The design and implementation of security technology is not a "casual thing", it takes time, care, a plan designed through a cross-functional team and the quality, integrity and craftsmanship of your business partner(s).

About the Author

Steven Nibbelink, CHPA, CA-AM, is the Business Development Manager of Healthcare for Vector Security Networks. Steven has over 20 years of industry experience and currently serves on the Board of Directors of the International Association for Healthcare Security & Safety Foundation. He is a member of IAHSS and earned his Certified Healthcare Protection Administrator (CHPA) in 2009; and has been recognized for outstanding contributions in the field of healthcare security and safety with the IAHSS Elwood Near Presidential Award in 2011.

About Vector Security Networks

Vector Security Networks (www.vectorsecurity.com/networks) is a division of Vector Security, Inc. a top 5 integrator of physical security solutions and managed services for North American businesses and multi-site enterprises, including many Fortune 500 companies. Vector Security Networks serves nearly 90,000 national account sites across North America.

About Vector Security

For more than 40 years, Vector Security, Inc. (www.vectorsecurity.com) has been a premier provider of intelligent security solutions tailored to the needs of the customer. Headquartered in Pittsburgh, the company offers a full suite of electronic security services for residential, business and multi-site customers across North America and the Caribbean through a network of branches and authorized dealers. Through Vector Security Networks, the company also offers customized managed broadband services that lay the foundation for unsurpassed business intelligence. Vector Security is a sister company of the Philadelphia Contributionship, a mutual insurance company founded in 1752, and currently provides cost-effective, technology-based security solutions to nearly 300,000 homes and businesses.

References

1 https://www.jointcommission.org/assets/1/6/SEA_WPV_TJC_requirements.pdf
2 Urgent Care Association of America (UCAOA) Accreditation Standards & Preparation Manual
3 https://www.osha.gov/Publications/osha3148.pdf
4 http://www.manmonthly.com.au/features/cctv-and-workplace-safety/
5 https://www.jucm.com/protecting-your-urgent-care-center-against-robbery/
6 https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#26f556431d09

VECTOR SECURITY® NETWORKS

2000 Ericsson Drive | Warrendale, Pennsylvania 15086