SUMMER 2017 | ISSUE 19

INSIGHT

FINDING THE RIGHT SOLUTIONS TO SECURITY

Innovation and common sense

PROTECTING OUR ASSETS

BUCHART HORN
ENGINEERS • ARCHITECTS • PLANNERS

NEXT

A MESSAGE FROM OUR PRESIDENT

Securing the integrity of our infrastructure assets is essential to maintaining national security and our way of life. A simple statement... but a very complex mission. This issue of *Insight* touches on efforts that go on behind the scenes every day to keep us safe. Often unnoticed, these efforts are required to neutralize the threats created by an ever-evolving world.

High priority in every design is the reduction of risk. We need to ensure our finished water is secured from the risk of contamination. We incorporate force protection into the development of critical structures to reduce the risk and impact of hostile acts. The educational system has incorporated multi-level security measures into the design of our nation's schools to prevent the unthinkable.

A great deal has been done over the last 15 years to secure our nation, but there is still much to do. This issue of *Insight* highlights just some of the improvements and innovation to our nation's infrastructure and technology that demonstrates our commitment to preparedness and risk reduction.

BRIAN S. FUNKHOUSER, PE, PRESIDENT/CEO

In this Issue

PREVIOUS

BUCHART HORN
ENGINEERS • ARCHITECTS • PLANNERS

is headquartered in York, PA with offices in
Louisiana
Maryland
Mississippi
New Jersey
Pennsylvania
Tennessee
Virginia
Germany

The Russell E. Horn Building
445 W. Philadelphia Street
PO Box 15040
York, PA 17405-7040

/company/buchart-horn-inc
/BuchartHorn
/BuchartHorn

(800) 274-2224
bucharthorn.com

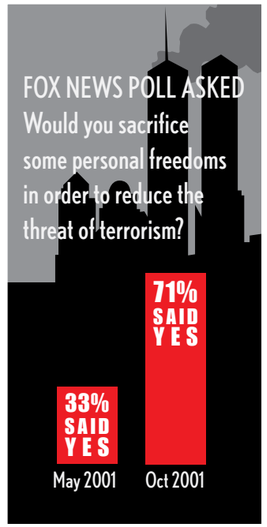
UNDER PRESSURE

BALANCING THE COST OF SECURITY AND CIVIL LIBERTIES

Most governments have some sort of critical infrastructure program in place to manage their assets that are considered essential for a functioning society and economy. The United States has had a program in place since 1996 to define these assets and offer guidelines on securing them. As technology has evolved and new risks have emerged, the Critical Infrastructure Protection Program has seen several notable revisions, including the 2013 US Presidential Policy Directive 21 (PPD-21). This adopted framework now recognizes the 16 critical infrastructures depicted on the back cover of this issue.

Striking a reasonable balance between security, civil liberties, and cost is a difficult proposition nations have always wrestled with. The PPD-21 program creates new regulatory and financial burdens upon the agencies and assets affected, approximately 85% of which are privately held. While advances in technology may reduce the cost to secure our assets, they may also infringe on personal civil liberties. Public opinion on this balance can shift dramatically after a tragedy or scandal, placing additional burdens on these assets to adapt security protocols quickly. The results of Fox News Polls conducted between 1996 and 2013 illustrate this perfectly. In May 2001, 33% of respondents were willing to sacrifice some personal freedom in order to reduce the threat of terrorism. The same poll conducted in October 2001 saw a jump to 71% of respondents willing to sacrifice some personal freedom. The catalyst being the terrorist attacks on September 11, 2001.

A number of factors can increase risk, such as the interconnectedness of sectors, the proliferation of exposure points, and a concentration of assets. For example, the United States has more than 4.1 million miles of public road. Although only 27% are located in urban areas, they become a chokepoint since they account for 67% of vehicle miles traveled . Crippling one of these chokepoints impacts the ability of several other critical sectors to respond quickly in an emergency. Given all of these risks, it's important for governmental managers to properly balance these risks with financial constraints and civil liberties of our citizens while working well with the private sector to manage all of these assets.



KEEPING US SAFE HAS ITS CAVEATS

TO TABLE OF CONTENTS

NEXT

SECURITY FOR THE BUILT ENVIRONMENT

FINDING WEAKNESSES AND DEVELOPING CORRECTIVE SOLUTIONS FOR OUR NATION'S OVERSEAS FACILITIES

Design for security is multi-faceted and requires a holistic approach to the building and its infrastructure. Physical attributes and functions, exterior (what is visible) and interior (what is invisible), must be assessed.

Security design has been one of the core competencies of BH's European office, Buchart-Horn GmbH, since 1985. Some of the customers we have provided security services to include US Department of State in Europe; US Army Corps of Engineers (USACE), Europe District; US Air Force Europe; Department of Defense Education Activity (DoDEA); Defense Information Systems Agency; Defense Threat Reduction Agency; and German government agencies and private industries. Security analyses, such as building and construction assessment, site development, facilities, and traffic planning, based on defined criteria are some of the key components. Security analyses including building and construction assessments evaluate key components such as site development, technology, and traffic planning while making recommendations to address security weaknesses and develop corrective solutions.

Buchart-Horn GmbH has a 30-year relationship with the US Department of State to solve the security issues of their consulates and embassies throughout Europe. On-site surveys and designs were provided for access control points (ACPs), standoffs, blast-resistant doors, walls, windows, perimeter security, fencing, active and passive barriers, common access cards, closed-circuit television, security lighting, and street layouts.

We have a long relationship assisting the USACE with upgrading security at their bases. Moving to address security concerns following the terrorist attacks of 9/11, the Headquarters, Department of the Army mandated Army installations worldwide adopt a closed post security posture and selected the USACE to establish an Access Control Point Program (ACPP) to deploy physical security equipment at all Army installations. They contracted Buchart-Horn GmbH to assist the USACE Europe District in Germany and throughout Europe. The objective was to provide physical and electronic security equipment to upgrade gate security and personnel safety and to reduce traffic congestion while maintaining Army standards for vehicular ACPs.

Buchart-Horn GmbH coordinated field surveys and reports of ACPs for more than 200 Army, and Air Force installations in Germany, Belgium, Italy, and the Netherlands. Thousands of variables were tracked as regulations and standards for ACPs were finalized. Buchart-Horn GmbH quickly became the subject matter experts using USACE Centers of Expertise and European Command Standards.

Amelia Earhart Building ACP at USACE Europe District HQ

Independent government estimates were prepared for the installation of approximately $20 million worth of security equipment throughout Europe. Architectural designs for ACPs include structural, mechanical, electrical, traffic, HVAC, security, and water/sewer considerations, along with construction plans, specifications, and cost estimates for various locations.

ACP components include large vehicle and privately owned vehicle inspection areas with canopies, visitor control centers, identification check areas with canopy and guard booths, guard houses, search offices, overwatches, denial barriers, and traffic flow control. At the US Army Garrison in Mannheim, Germany, Buchart-Horn GmbH analyzed antiterrorism force protection (ATFP) and blast resistance for 16 buildings. Stand-off distances, structural deficiencies to withstand potential explosive forces, egress routes, sight-lines, and personnel refuges were addressed with corrective measures to protect the installation and people. Upgrades involved structural and non-structural changes. ATFP surveys and projects were also performed for DoDEA Europe for elementary, middle, and high schools.

Buchart-Horn GmbH was opened in Frankfurt, Germany in 1985. With 30 architects, engineers, and planners, the German team focuses on providing innovative architectural design services for the United States' federal government and boasts an impressive portfolio of design work that includes US military installations, consulates, and embassies throughout Europe. We are proud to bring our experience and expertise to protect our nation's personnel and facilities.

Photos on video screens: 1. ACP Design, Artillery Kaserne, Germany, 2. Amelia Earhart Building ACP, at USACE Europe District HQ, 3. US Embassy, Bratislava, Slovakia CAC, 4. US Consulate, Hamburg, Germany, 5. Perimeter Security, Den Hague, Belgium, 6. US Consulate, Munich, Germany

CALEA-accredited Lower Allen Township Municipal Services Center

CALEA-accredited Derry Township Municipal Complex

TO SERVE AND PROTECT

by W. Scott Loercher, AIA, NCARB, LEED AP BD+C

Modern police facilities use layers of security, incorporating technology and design to fashion facilities that are community-oriented, yet completely secure for employees and visitors. The dangerous truth is many police stations across the country are outdated and lack sufficient security measures such as bullet-resistant materials, metal detectors, and adequate security access controls. While these measures can be retrofitted into existing design, it is most effective when integrated into the design of the facility.

Community Integration

When designed correctly, security shouldn't be the first thing you notice when you walk into the building. Security should be just another component of the facility that is functional and doesn't draw attention to itself. De-escalation of conflict starts with proper design and understanding the symbolism of the modern police facility. No longer glorified bunkers, public safety facilities must instead be beacons of safety that symbolically and physically act as the center of a community. They need to appear transparent, consider the cultural and historical context of their location, and have the ability to be safe havens in crises. Creating the perfect balance between warmth and security is paramount.

Deterrents such as video surveillance and metal detection are obvious choices and can be added to any new or existing facility. They serve as top-of-mind security measures. While other security measures are more subtle or even unseen, such as bullet-resistant glazing and in-wall ballistic resistant panels. The traditionally open public lobby can incorporate baffles into the security glazing to allow for direct communication with the public. This feature is often more inviting than a speaker hole, a microphone, or call box. Bullet-resistant fiberglass panels installed into station walls, ceilings, and counters can cover drywall or tile to keep a traditional look.

Soft interview rooms adjacent to the lobby are used for people reporting crimes or to separate individuals during questioning. These rooms are designed to make adults and children feel relaxed and safe. It is paramount to create a safe space for the person reporting domestic violence or an assault so they don't feel victimized while talking to officers or giving statements. Interview rooms used for suspects or individuals in custody are more secure and less welcoming.

Limiting Access

Access control starts at physical checkpoints throughout the building. Full-height interior partitions provide the physical barriers that separate secure spaces. Electric door access allows departments to limit access and create a record of entry. For evidence processing and storage areas, two levels of security are recommended to limit unauthorized use. Fingerprint and voice recognition are two of the more common means to compliment traditional key fob or card readers. Many door access systems have the ability to record who and when users accessed the space and may provide a request to exit device when leaving the space. Electronic control systems allow owners to quickly and easily add and remove authorized users, no longer requiring expensive lock cylinder replacement or dealing with the threat of lost or duplicated keys. Access points typically monitored include interview rooms, evidence storage, juvenile holding rooms, armories, and equipment rooms.

Every Detail Considered

Consideration of how employees and the public will use the facility is a vital safety consideration. Interview rooms can be accessible from two sides—from the public lobby and from the police side where only authorized personnel can enter or leave. An interview room's soft security is built into the design. Light fixtures are security grade and flush with the ceiling, so they cannot be used as weapons. If there is an altercation and an officer is knocked to the floor, alarm bars are located at floor level to call for assistance. Exterior design considerations include a standoff distance to help with perimeter security. It is designed to protect personnel inside the building from vehicle threats. Landscaping or barrier systems can be designed in the architecture and landscape to coordinate with building aesthetics.

PREVIOUS

"De-escalation of conflict starts with proper design and understanding the symbolism of the modern police facility."

Another successful tool used to provide a secure facility is using Crime Prevention Through Environmental Design (CPTED). CPTED is defined as a multi-disciplinary approach to deterring criminal behavior through environmental design. CPTED strategies rely upon the ability to influence offender decisions that precede criminal acts by affecting the built, social, and administrative environment. CPTED guidelines provide practical solutions that can be tailored to the unique needs of agency facilities.

Accreditation

Accreditation is a progressive and time-proven way of helping institutions evaluate and improve their overall performance. The cornerstone of this strategy lies in the endorsement of standards containing a clear statement of professional objectives. Buchart Horn Architects offers a free evaluation of agency facilities based on requirements set forth in national and state accreditation guidelines. The evaluation provides the agency an understanding of what limitations are present at their current facility and provides recommendations for removing obstacles that may prevent accreditation.

While each state may have their own standards for accreditation, the Commission on Accreditation for Law Enforcement Agencies (CALEA) has become the national standard for an agency to voluntarily demonstrate their commitment to excellence in law enforcement. The standards upon which the Law Enforcement Accreditation Program is based reflect the current thinking and experience of law enforcement practitioners and researchers. Major law enforcement associations, leading educational and training institutions, and governmental agencies acknowledge accreditation programs are essential to the development and success of professional law enforcement agencies.

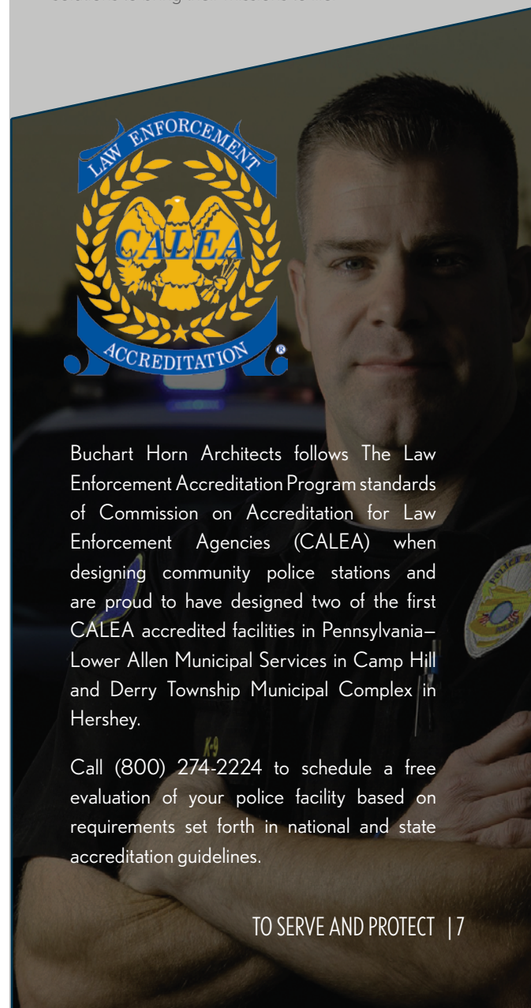
Becoming an accredited department can limit an agency's liability and risk exposure because it demonstrates that internationally recognized standards for law enforcement have been met and verified by a team of independent outside trained assessors.

"Becoming an accredited department can limit an agency's liability and risk..."

TO TABLE OF CONTENTS

NEXT

Scott Loercher, Vice President of Architecture, is responsible for providing design leadership by providing clients with unparalleled service, continually striving to improve the quality of the firm, and imparting exceptional design while creating meaningful places where communities can thrive. Throughout his career, Scott has specialized in turning clients' visions into extraordinary architecture by collaborating with leaders of public and private organizations, helping them articulate their goals, and following through with design solutions to bring their missions to life.



Buchart Horn Architects follows The Law Enforcement Accreditation Program standards of Commission on Accreditation for Law Enforcement Agencies (CALEA) when designing community police stations and are proud to have designed two of the first CALEA accredited facilities in Pennsylvania—Lower Allen Municipal Services in Camp Hill and Derry Township Municipal Complex in Hershey.

Call (800) 274-2224 to schedule a free evaluation of your police facility based on requirements set forth in national and state accreditation guidelines.

PROTECTING THOSE IN BLUE

LEVEL 6

EVIDENCE: Departments may have several ways to handle/process evidence. While larger departments may have more volume, each department requires space to process and store evidence. Temporary evidence lockers are a good way for officers to quickly secure evidence when entering the department. When space permits, they provide an area for officers to record, package, and label evidence. The evidence technician can remove the evidence at a later time for further processing or storage. Consideration should be given to large, bulky items and even vehicles.

LEVEL 5

HOLDING: At a minimum, a department should have a secure room for interviews and short-term holding. Secure rooms can use abuse-resistant wall board with security grade fixtures, doors, and hardware. When providing individual holding rooms, departments should consider separating genders and juveniles. Separation of individuals should include limiting visual contact and sound between holding areas.

LEVEL 4

POLICE ACTIVITIES: This is typically the largest area in the department. Major spaces include squad or patrol space, administrative offices, locker rooms, equipment storage, and meeting rooms. Open office space may have direct access to all other levels, requiring the area to be secure from civilian employees and should not provide any danger to officers when escorting individuals in custody.

LEVEL 3

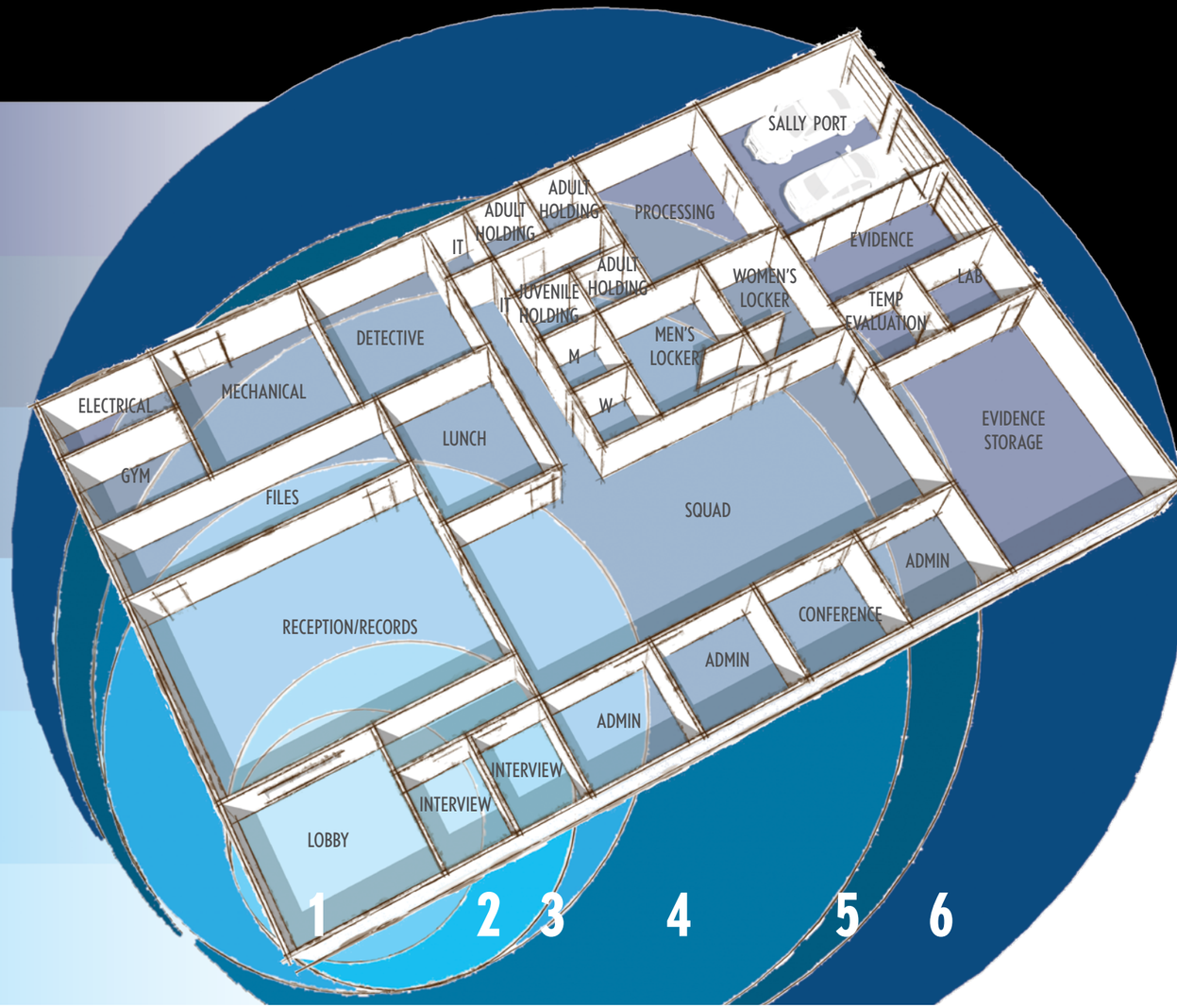
NON-SWORN EMPLOYEES: This typically includes administrative-assistant level positions but can also include public safety dispatchers, Community Service Officers, or Public Service Technicians in larger departments. The space includes traditional office configuration with immediate access to files, public lobby, and squad room. Access may also be needed for investigative duties and evidence processing.

LEVEL 2

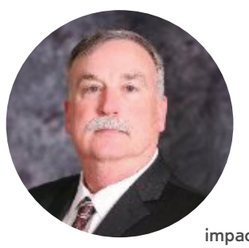
INTERVIEW: Usually a semi-secure, quiet room located with direct access to the lobby and/or squad area, this conflict resolution room is used for private interviews with the public. The space is used to help diffuse aggressive speaking individuals and, when more than one are available, they can be used to separate couples or small groups. Sound attenuation and electronic hardware is recommended.

LEVEL 1

PUBLIC: Entry lobby for visitors entering the facility; may be shared with other community services. Levels of lobby security vary from open counters and face-to-face communication to impact-resistant glazing and ballistic panels. When ballistic ratings are requested, it is important to rate all publicly accessible walls separating public space from employee space.



Designing a facility that protects the public, those in custody, and our law enforcement members requires levels of security that ensure sought-after accreditation



Frank E. Williamson, Jr., Director of Public Safety/Assistant Township Manager, Lower Swatara Township (Former Chief of Police/Director of Public Safety at Lower Allen Township)

Q&A

What seemingly simple security design element plays a more impactful role than the public may assume/be aware of?

Access control through card access and biometric readers.

What security measures/design elements do you find the most vital to protecting evidence and chain of custody?

Double authentication for access, motion sensing cameras on the entrance/exit, and a separate alarm system (motion/door break).

What benefits do you see to having state/national accreditation for your facility?

Accreditation standards give you the WHAT – the WHAT is contained within the standard. This leaves the HOW up to the agency – HOW the facility or procedures are used to meet the WHAT of the standard. Accreditation gives you a best practices guide, and the agency must meet or exceed those standards in order to be accredited. It also requires constant review, revision, and improvement. It forces you to look at the hard issues and overcome them.

Is there a reduction in your liability for being an accredited facility?

Not for just the facility, but the facility and the security measures are all a part of the state and international accreditation process. Some insurance agencies in Pennsylvania will give you a discount for being PLEAC [Pennsylvania Law Enforcement Accreditation Commission] accredited. Most insurance carriers will give you a discount, some as much as 25%, for being CALEA accredited.

In order to receive state/national accreditation, police departments must adhere to standard operating procedures (SOPs). What facets of your facility help you adhere to those SOPs?

Mainly, the physical plant security and preparedness. Security and facilities for evidence and firearm/ammunition storage and accountability. Ensuring back up power, ensuring there is physical security for facility and law enforcement area access, proper access to potable water, and restroom facilities for holding/detention areas.

Todd Vukmanic has more than 21 years of experience providing conceptual design and programming of K-12 facilities from initial feasibility study and evaluation, through schematic design and design development, as well as final construction documentation and building analysis.

SAFE SPACES

DESIGNING A SECURE ENVIRONMENT FOR LEARNING

by Todd J. Vukmanic, Associate AIA

What is your philosophy on designing K-12 facilities?

It's very interesting how the educational approach has evolved over recent years. Teaching trends currently focus on student interaction and collaboration in the classroom, with an emphasis on interactive curriculum and flexible learning spaces. Likewise, security within these schools is more imperative than ever. Implementing security measures within the overall building design, from the inception of the project, is critical. At the end of the day, educational facilities should be designed to integrate security measures and provide for flexibility and expansion to accommodate the current and future educational curriculum.

What makes K-12 design different than other architectural designs?

Educational design, like many others, focuses on solving the design program. It also involves incorporating the required educational plan set forth by the school district. But unlike many other designs, educational design must also anticipate changes and progression in educational curriculum and student learning methodologies. Technology is rapidly advancing. Instructional techniques are evolving. Educational curriculum is being revised and implemented more often than ever. All of these shifts in the way students learn and instructors educate have a direct impact on the way these facilities are planned and conceptualized.

What are some challenges you face when designing K-12 facilities?

The purpose of any educational design strategy is creating innovative and progressive buildings that support flexible learning and student autonomy, while providing secure educational facilities for both students and educators. The focus is to create open and transparent spaces that promote positive learning environments and enhance natural surveillance and security. Therefore, the biggest hurdle I've experienced is finding the proper balance between creating open and inviting educational spaces, while maintaining a high level of security and control. Designing spaces that foster the student and educators learning process, yet also maintaining the safety and supervision that is expected in this type of facility.

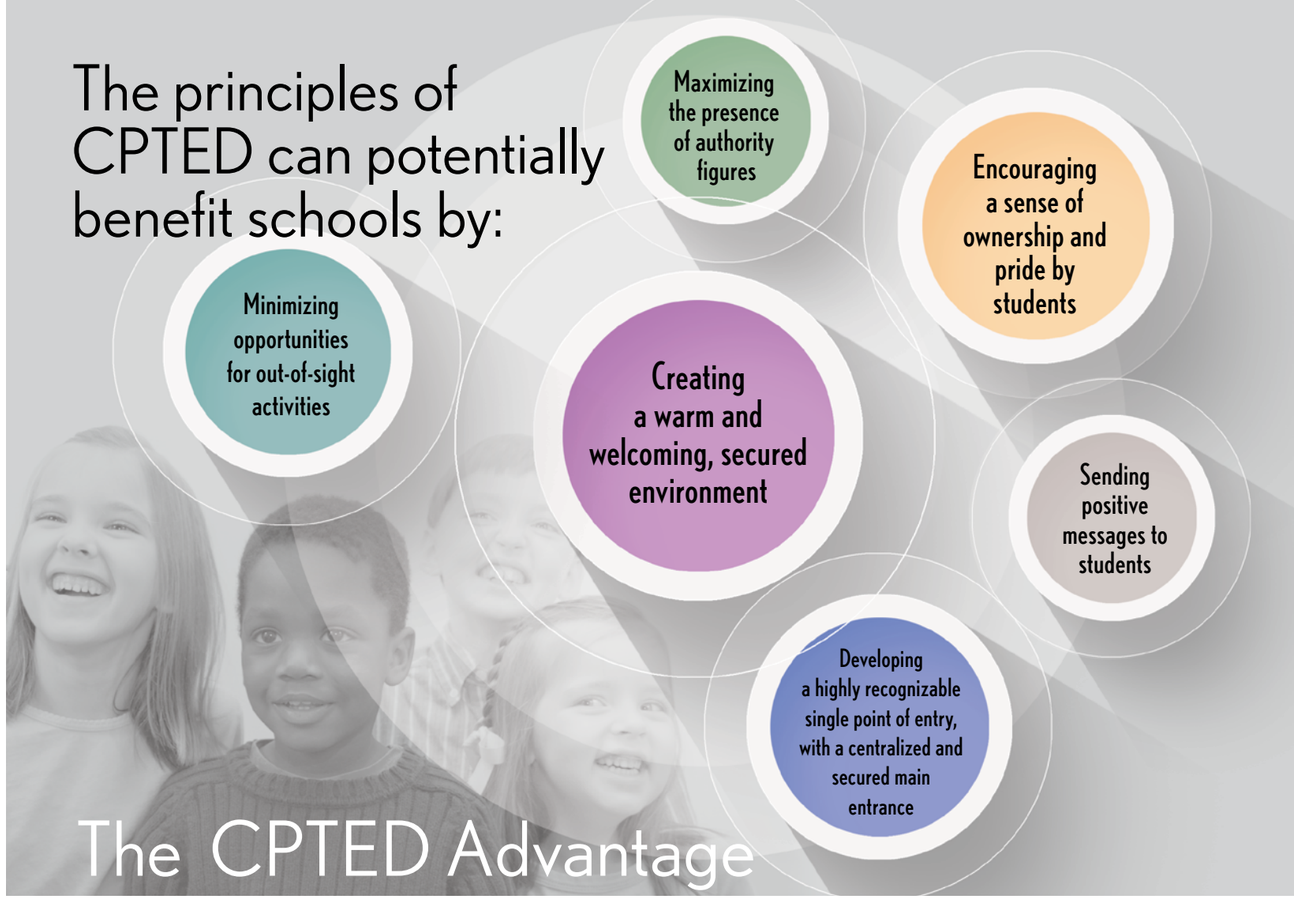
Security is critical when designing K-12 facilities. Are there standard security measures implemented in every K-12 design?

The short answer is: "there should be." Oftentimes, it can be difficult to execute an overall security design concept throughout an existing facility. Implementing security design tactics such as layering and building compartmentalization can be difficult to accomplish by maintaining exiting and travel distances, while avoiding dead-end corridors. However, there are several standard security design tactics that should be considered in every educational facility. These strategies should be implemented, when possible, during the conceptual design phase. They include such approaches as layering and target hardening, improved surveillance and visibility, defined entry and access control, and safe school planning. These security protocol tactics improve the overall safety of the facility, while effectively reducing the likelihood of an incident.

What is your insight on the future of Crime Prevention through Environmental Design (CPTED)?

Unfortunately, CPTED design methodology is still widely unknown and underutilized by the design community. Oftentimes they are simply a consideration after the building design is completed or only a cursory afterthought with a few minimal tactics implemented throughout the facility. It would be my hope the procedures involving CPTED design protocol would be incorporated from the inception of the building program as a holistic design approach. The integration of CPTED protocol into the overall facility systems and building infrastructure should be a major consideration by the design community. These procedures should be as mandatory as building code and life safety, in the development and compliance of the design project.

PREVIOUS



Not only must educators prepare our children for the future, they must keep them safe from possible threats. While schools in the United States are relatively safe, any amount of violence is simply too much – and sadly, we're all too familiar with school tragedies. During each school day, our nation's schools and educators are entrusted to provide a safe and healthy learning environment for approximately 55 million elementary and secondary school students in public and nonpublic schools.

When designing and developing a facility, addressing security measures is imperative. Oftentimes, enhanced security methodology can be incorporated into the overall design from the inception. The system by which safety and security standards are prioritized is called Crime Prevention Through Environmental Design (CPTED), the internationally accepted multi-disciplinary approach to deterring criminal behavior through environmental design.

CPTED PRINCIPLES

- **Territoriality** – involves an individual's perception of, and relationship with, the environment. A strong sense of territoriality encourages an individual to take control of his or her environment and defend it against attack.
- **Surveillance** – principal weapon in the protection of a defensible space. Criminals are least likely to act when there is a high risk of their actions being witnessed.
- **Access Control** – influencing and controlling how people interact with the space, denying access to a crime target and creating a perception of risk to the offender.
- **Target Hardening** – increasing the effort that the offender must take to conduct the crime.
- **Image/Maintenance** – repair and general upkeep of space.
- **Activity/Support** – increases the use of the environment for safe activities with the intent of increasing the risk of detection of criminal and undesirable activities.

Sources: US Department of Education, Office of Elementary and Secondary Education, Office of Safe and Healthy Students, Guide for Developing High-Quality School Emergency Operations Plans, Washington, DC, 2013

Youth Violence: Using Environmental Design to Prevent School Violence. Centers for Disease Control and Prevention. Centers for Disease Control and Prevention, 02 Aug. 2016. Web. 02 Mar. 2017.

TO TABLE OF CONTENTS

NEXT

FROM EXPOSED AND VULNERABLE...

TO COVERED AND PROTECTED

ENCLOSED FROM MAN AND NATURE

Protecting Baltimore's precious water supply from threats

Part of the greater Baltimore area's finished water storage was handled by the uncovered 21 million gallon Pikesville Reservoir located adjacent to the Baltimore Beltway Inner Loop. In order to protect its water supply from natural and man-made contamination (both accidental and deliberate) and to replace an 80-year old structure in poor condition, it was imperative to replace the open reservoir with covered facilities. Covered water storage facilities protect finished drinking water from organic contamination such as leaves, insects, or animals. The main concern is bacterial contamination from wild animals and humans as well as intentional tampering from terrorists or anyone wishing to disrupt a reliable supply of safe drinking water.

BH helped Baltimore County and the City of Baltimore replace the uncovered Pikesville Reservoir with two giant enclosed finished water tanks. A 5 million gallon tank was first constructed adjacent to the existing reservoir and put into service. The existing reservoir was then demolished and a 15 million gallon tank was constructed in its place.

The new covered, finished drinking water facilities provides metropolitan Baltimore with a safe and reliable storage asset for its water system customers well into the future.

PREVIOUS

SECURING ONE OF OUR MOST PRECIOUS RESOURCES...OUR WATER

The water industry faces unprecedented challenges posed by numerous threats that could compromise our access to safe drinking water. Environmental threats such as airborne contamination or pathogens, direct contamination of supply sources (either deliberate or accidental chemical spills), and cyber attacks directed at critical equipment operated by industrial control systems are all present and, in some cases, occurring more frequently. Interest in cyberattacks has grown, especially over the past year, with the first suspected cyberattack of a utility occurring in the Ukraine in 2015, disrupting electrical service to more than 225,000 customers.

You might ask, "what are public and private water providers doing to protect our drinking water systems?" The answers to the question are more easily understood if broken into several components: detect, delay, and respond. The area of detection is probably the most rapidly growing area as technological advances are quickly emerging onto the security scene.

While cameras and surveillance systems comprise a large part of the technology being applied to detect physical attempts for intrusion, advances in fiber optics have been used to detect movement in areas not easily secured by perimeter fencing, as one example. Fiber cables can be buried in the ground to detect movement, discriminating down to the type of vehicle or differentiating between a person and an animal. Detection can also be applied to cyberattacks. Advances in IT technology have resulted in new appliances able to detect illicit intrusions or unusual activity and an IT system using pattern recognition.

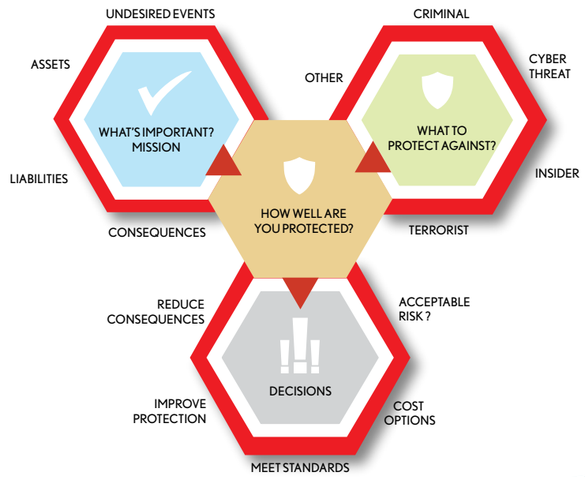
Any physical barrier, network, or security system can be breached if enough time is available. Thus, it is imperative water treatment plant operations consider where risks to operations might exist and mitigate that risk by delaying that breach. Combining several layers of defensive barriers (i.e., locks, fencing, card reader access systems) with detection, augments the overall security posture of an operation. IT professionals use technology called "honeypots" that draw attention to an inert location in an IT system, delaying and diverting a hacker's attention away from more lucrative control system targets.

A critical element of any security system is the ability to respond. What happens if a chemical detection upstream of a supply intake triggers an alarm? Can systems be manually controlled to shut off intake valves to avoid bringing a contaminant into a treatment plant? Can malware be isolated within an IT system before it attacks the controls to pumps or motor controls? The responses put in place either through technology or well-defined methods of operation often dictate how much damage will be avoided if the detection and delay components were breached.

No security system is impenetrable and any approach to securing a water treatment plant or associated storage or distribution systems must use a multi-layered approach. A security assessment is a smart way to address each of the threats, including cyberattacks, and smart guides have been published to assist in evaluating your own security.

A good first step is to prioritize what facilities are most critical to the operation of the system and develop a plan to best protect those assets. After the terrorist attacks of September 11, 2001 all water utilities were required to conduct vulnerability assessments that effectively analyzed each system and ranked the critical assets based on criteria developed by the utility. The method used to analyze water utilities, Risk Assessment Methodology for Water Utilities (RAM-W), is depicted here. In many cases the most valuable asset is clear to the utility, but the value in ranking all of the assets is in knowing where they stand with respect to each other. Once the utility has a prioritized list of assets to protect, they can begin determining if operational changes can be implemented to secure the assets and where best to invest in capital improvements to reduce vulnerabilities.

Risk Assessment Methodology for Water Utilities (RAM-W)



TO TABLE OF CONTENTS

NEXT

David T. Lewis, PE, Vice President and General Manager of Columbia Water Company, has more than 27 years of engineering experience involving a variety of potable water, wastewater, and environmental projects. He received a Bachelor of Science in Environmental Engineering Technology from The Pennsylvania State University. He is a licensed Professional Engineer and water and wastewater operator.

Strategically placed monitors scan the facility 24/7

SECURITY CHALLENGES ABOUND

Using Risk Management to secure our water supplies

Q&A

What do you see as the biggest security-related challenges facing the water industry?

Dave: The biggest-security related challenge is cyber security. The need for automation and remote monitoring and control is driving the industry to rely more and more on networks and computer systems. Keeping these systems private and away from actors who wish harm is an ongoing challenge.

How has the Department of Homeland Security's (DHS') National Infrastructure Protection Plan (NIPP) impacted your operations?

Dave: The DHS NIPP has not impacted us directly; however, the PUC [Pennsylvania Utilities Commission] and DEP [Department of Environmental Protection] have implemented new regulations and regulation changes as a result of that plan.

We see the term risk management being used in the context of securing our water supplies. Can you expand on how Columbia Water Company uses risk management to decrease security threats to its processes or sources of supply?

Dave: Securing our water infrastructure is one of the most important things we do on a day-to-day basis. The types of threats are endless which makes it difficult to avoid everything at all times. We found that the key is to install infrastructure that allows you to manage those risk effectively. We are currently in the process of installing security fencing, door, hatch and ladder monitors, and security cameras at all of our critical locations. This security equipment allows us to identify and react to threats in nearly real time.

PREVIOUS

> Securing our water infrastructure is one of the most important things we do on a day-to-day basis.

A series of catwalks ensures access to critical components in the event of flooding

Tank tie downs and portable flood panels provide cost-effective flood protection

Founded in the mid-1800s, the Columbia Water Company (Columbia) operates the historic Walnut Street Water Treatment Plant (WTP) located along the Susquehanna River. The WTP features several structures on the state's Historic Register dating back to 1849 and is located in the flood plain. While several mitigating strategies have been implemented over time to minimize flooding impacts, Columbia recognized the unique historic significance and landlocked nature of the WTP necessitated innovative approaches to meet increasing demands and enhance operational resiliency, especially during flood events.

To continue to provide high quality drinking water, improve plant flexibility and resiliency, and meet new state and federal regulations, Columbia turned to BH to meet their needs. The three-year, multi-phase project provided a highly efficient, cost-effective plant, doubling the potential capacity to 6 MGD.

The project featured the evaluation of existing equipment and treatment processes, along with research for solutions to fit capital and operating budgets while adapting to the historic site constraints. BH evaluated the raw water intake and pumping station, the chemical feed system, the flocculation and sedimentation system, sludge control collection system, filtration, clearwells, emergency power, and the SCADA system. Evaluations considered material types, equipment locations and efficiency, and architectural/historic elements requiring unique designs for the building envelopes and ventilation systems. Following the field assessments, BH created schematic through final designs while coordinating equipment and treatment process relocations within existing or modified structures. Our solution complies with historic preservation requirements while enhancing the WTP's safety, efficiency, and resiliency.

Redesigned floodwall replaced rubble barrier to complement historic setting and protect the facility

TO TABLE OF CONTENTS

NEXT

2017 Diamond Honor Award for Engineering Excellence from the American Council of Engineering Companies of Pennsylvania (ACEC/PA): Diamond Awards recognize Pennsylvania engineering firms for projects that demonstrate a high degree of achievement, value, and innovation, according to ACEC/PA.

BUCHART HORN
ENGINEERS · ARCHITECTS · PLANNERS

The Russell E. Horn Building
445 West Philadelphia Street
PO Box 15040
York, PA 17405-7040

(800) 274-2224
bucharthorn.com

VISIT US ONLINE

Visit bucharthorn.com to learn more about our capabilities and projects completed.

THE 16 US CRITICAL INFRASTRUCTURE SECTORS

Partnerships that require diligence

Because the private sector owns and operates a vast majority of the nation's critical infrastructure, partnerships between the public and private sectors that foster integrated, collaborative engagement, and interaction are essential to maintaining critical infrastructure security and resilience.