Cybersecurity
How to stop 98% of threats

Continuity Planning
Enhanced security can make the difference

School Security
2 views on how to keep children safe

SIA

Insights

TECHNOLOGY

Volume 2, Issue 2
Winter 2014-15

SIA Technology Insights is published twice a year by the Security Industry Association. All editions are available at www.securityindustry.org/techinsights. For information about submitting or republishing articles, contact Ron Hawkins at (301) 804-4713 or rhawkins@securityindustry.org.

Publisher: Don Erickson
Editor: Ron Hawkins

Welcome

Dear Reader,

Looking through this edition of *SIA Technology Insights*, it is interesting to see the themes that – unintentionally – emerge.

You will, for example, see multiple writers caution against taking a "one-size-fits-all" approach to security. You will also see more than one warning about the "insider threat." And you'll read several times about the critical need to have equipment and procedures in place to verify the identities and access needs of personnel in given locations. You will probably find a few more common threads yourself.

All of this serves as a reminder that, even though we are competitors seeking the best for our individual companies, we share the same ultimate goal – protecting people and property. Our industry has developed some extraordinary solutions to do just that, and we are proud to have the opportunity to showcase many of them in this publication.

We hope you enjoy reading about the security technologies and strategies featured in the following pages, and we invite you to submit comments and suggestions to the editor of *SIA Technology Insights*, Ron Hawkins, at rhawkins@securityindustry.org.

And remember that you can read digital versions of all issues of this publication at www.securityindustry.org/techinsights.

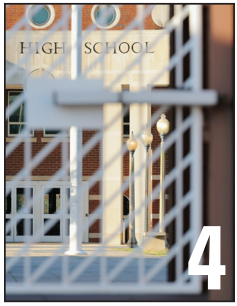
Thank you for reading.

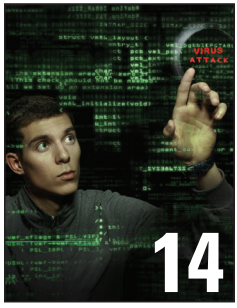
Sincerely,

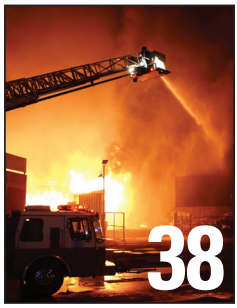
V. John Stroia
Chairman, Board of Directors
Security Industry Association

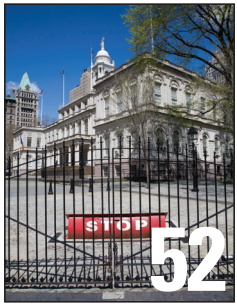
Don Erickson
CEO
Security Industry Association

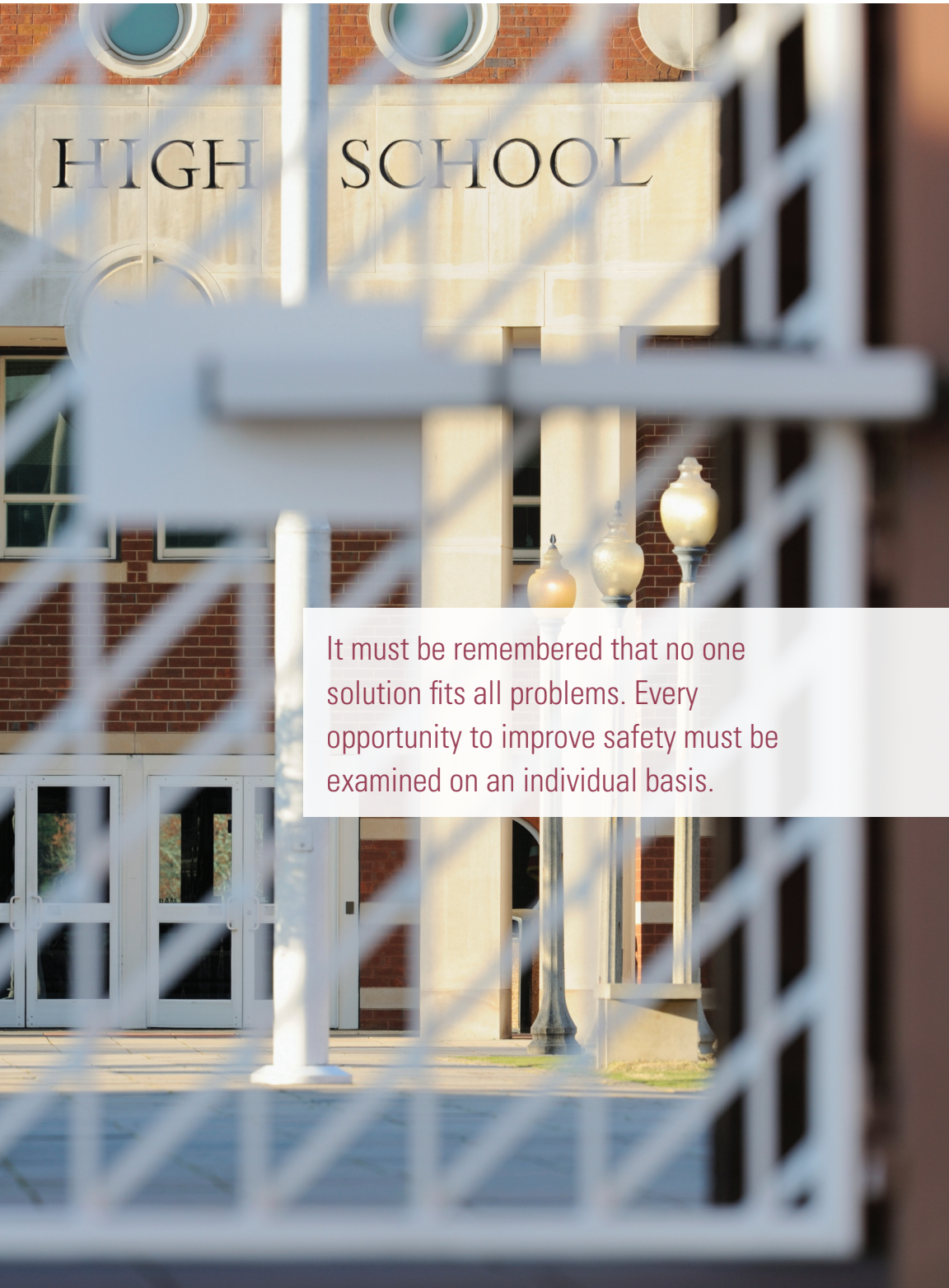
Table of Contents











It must be remembered that no one solution fits all problems. Every opportunity to improve safety must be examined on an individual basis.

Get Up and Bar the Door

Access management and door hardware play a critical role in school security

By **April Dalton-Noblitt**,
Director
Allegion

"We need to protect our children from shooters." So read the headlines. So demands Congress, the governor, the mayor, the chairman of the school board, the principal and every parent. So the maintenance staff at a school makes a fix that will keep the shooters out but, in doing so, will unintentionally enhance the opportunities for a score of other safety and security breaches. In other cases, staff members simply use the wrong types of solutions, ones that actually create more problems than they solve. As security professionals, we need to offer our services to prevent such errant "fixes."

Did you know that student-on-student and student-on-teacher violence is more likely than an outside intruder causing harm? The U.S. Department of Education and the U.S. Department of Justice report that, in 2010, there were approximately of age, and approximately 7 percent of teachers say that they have been threatened with injury or physically attacked by a student. Overall, it is about 30,000 times more likely

that a student or staff member will experience a non-fatal violent crime in school than a fatal attack.

Real Solutions for Access Control

Access management involves guiding people, or managing human traffic, with signs and well-marked exits. It also includes subtle tactics like using landscaping to limit access to unsupervised locations on facility grounds.

Lower-cost mechanical solutions like high-security keys can help control access to places like storage, equipment and utility rooms.

Problem Areas in Access Control

There are several common security shortcomings that should be identified and addressed when improving access control in schools:

- Door hardware that forces an individual to step out of the room to lock the door, exposing that person to danger in the hallway.
- Hardware with "unrestricted ability" to lock or unlock the door. This lets anyone – including students – take control of an opening.
- Magnets or tape on the door to prevent latching. Not only is this a violation of the fire code but it also makes lockdowns more difficult.
- School doors that don't automatically close, potentially preventing them from being in a ready position during a lockdown.
- Hardware that is not permanently attached to the door, requiring staff to locate and attach the device in the midst of a lockdown.
- Hardware that slows access or egress during an emergency situation.
- Deadstop devices or sleeves that clasp around the v-shaped hinge attached to the closer mechanism on doors. This is another violation of the fire code.
- Floor bolts or other devices that obstruct the door and prevent it from closing.
- Anything that blocks emergency responders from entering.
- Anything that might be used by an unauthorized person acting with ill intent.

When selecting security hardware and establishing security protocols within a school, school administrators should consider several things, including:

- Severity of risk
- Probability of risk
- Effectiveness of mitigating risk
- Ability of staff to implement lockdowns
- Budget

Electronic access control solutions – whether standalone or networked, wired or wireless – deliver enhanced security with an audit trail that lets administrators see who has entered a given area and when.

There are many ways in which schools can improve their access management. For example:

- Assign visitors a badge or name tag when they enter the building and require it to be returned before leaving.
- Keep staff and public parking separate from the areas designated for bus unloading and student drop-off. Make sure signage clearly identifies these areas.
- Keep all exterior doors locked during school hours, with the exception of the main entrance, to prevent people from entering the building without the office staff being aware.

Miller Place Union Free School District in New York went a step further and created a controlled single entry point for visitors. At most schools in the district, a secure vestibule was set up in close proximity to the office. Visitors must present identification before being allowed to enter. At a school where it was impossible to construct this type of entry, a visitor must be identified before being allowed to enter a locked door.

Upon entry, a visitor must present a driver's license to be scanned. For future visits, the person's information is maintained in a database, enabling

identity verification. Other data can also be stored, such as custodial parent issues or security concerns that would affect granting or denying future access.

At the San Mateo Union High School District in California, a combination of relatively simple but effective access control solutions protects students, teachers and staff with minimal system management requirements. The district controls door access with a key system. Keys are only available to authorized individuals through professional locksmith channels, which helps prevent unauthorized key duplication, and the keyway is exclusive to the district within a specified geographic area.

The Cobb County School District, the second-largest school system in Georgia, upgraded access at its elementary schools with a card system that simplifies access management and reduces maintenance costs. Formerly, access to all schools was controlled by mechanical keys and, as often happens, there got to be so many keys that the

district had a difficult time keeping track of all of them.

To determine whether electronic access control was feasible, the district conducted a pilot program at one elementary school, installing proximity card readers and electric latch retraction exit devices at the five most-used entrances. All other exterior doors were locked and monitored. After the pilot program proved successful, the system was installed throughout the district. Controlled doors are unlocked and relocked according to schedule during school hours. Holidays are accounted for, and unscheduled closings are easy to program.

> In some cases, staff members use the wrong types of solutions, ones that actually create more problems than they solve. As security professionals, we need to offer our services to prevent such errant "fixes."

It is easier to issue and delete credentials with card access than it is to issue new keys and get them back when someone leaves. Deleting a lost card also is considerably less expensive than rekeying multiple doors. In addition, cards can be programmed to operate for a limited time or for specific hours to control access for contractors or others.

To make it even easier on students and staff, some schools are moving to a new credential. As near field communication (NFC) technology is added to a growing number of mobile devices to enable access control, payments and other applications, more and more organizations are considering joining the "bring your own device" trend and having their users deploy their smartphones as their access control credentials. NFC provides communication between two devices that are in close proximity to each other, usually no more than a few inches, with the same security as using a smart card.

Since November 2011, Villanova University students and staff have been using a web-based service along with NFC and their smartphones as their ID to access dormitories, academic buildings and administration offices. Students download an app to install their one-card credential to their phone. To use the credential, they simply open the app and present the phone to the reader. Access is quick, easy and secure. Among the students in the Villanova trial, more than 70 percent said they prefer to use their phone, rather than a badge, to enter buildings.

The Right Products in the Right Places

First, it must be remembered that no one solution fits all problems. Every opportunity to improve safety must be examined on an individual

basis. Whoever is leading the charge – whether integrator, locksmith or administrator – needs to know that there are specialists who can help them. One important person to contact is a specification writer who can advise them or write the specification for them. Putting the correct code-compliant products in the right places increases school safety.

Main Entrance

Many schools restrict access via the main entrance during school hours. While students enter or leave school at the beginning or end of the day, the doors are typically unlocked. At these times, most schools have additional staff at the entrance to help monitor access. During school hours, doors are locked and a camera monitors who rings the bell for access. Office personnel assess the visitor and allow access, if appropriate. As a second line of defense, as noted above, some schools also deploy an entrance vestibule that directs visitors to the office. Electrified hardware on these openings facilitates immediate lockdown.

Secondary Entrances

Often, there are entrances from the parking lot or playground used by

teachers and staff. Electronic access control is typically recommended for these entrances, allowing the time of access to be controlled and monitored. Entrance is via a keypad and PIN or reader and card credential. The days of giving keys to half the town for after-hours use are over (or, at least, should be).

More and more organizations are considering joining the "bring your own device" trend and having their users deploy their smartphones as their access control credentials.

Emergency Exits

These are additional doors that are not required for access but do provide free egress. These doors are often "exit only" with no exterior operating hardware, although some facilities prefer a key cylinder on the exterior to allow quick access for emergency personnel. These doors are often monitored so staff can see if they are closed and latched. They can be automatically monitored as well, providing an alert if open. Additionally, visual status indicator options for exit devices and locks provide an at-a-glance verification of the locked/unlocked status of the door. Staff, then, can easily identify if the door is locked and can quickly secure the door's exit device or lock if it is not.

Classrooms

In many school violence incidents, lives have been saved because of locked interior doors. Whether students

and teachers hid in closets, bathrooms, storage rooms or locked classrooms, the doors provided critical protection. Classroom security locks have been standard in many school specifications for years, not just for classrooms but for just about any room that would have had a regular classroom function lock in the past. These locks let a teacher lock the outside lever without opening the door. An indicator on the inside rose or escutcheon that confirms that the outside lever is locked is extremely helpful.

Assembly Spaces

Large spaces like gymnasiums, auditoriums, cafeterias and libraries typically have doors equipped with panic hardware or fire exit hardware. These devices may be equipped with cylinder dogging or a trim control that is similar to a classroom security lock, allowing the doors to be locked without entering the corridor. To facilitate a quick lockdown of a bank of doors, staff may want to limit access to one door or door pair while keeping the others locked on the pull side. If budget allows, electric latch retraction provides immediate lockdown of these doors.

Watch out for "innovative" new products designed to make schools safer. Although these products may be based on great ideas and good intentions, many are not code compliant.

Door hardware, including exit devices, locks and closers, usually take a beating in schools and other facilities. Conducting regular maintenance checks will ensure that these components continue to operate properly, so that doors latch securely and open and close smoothly to enable fast lockdown or egress when needed.

Electronic security technology may also require software updates, reprogramming after personnel

changes, battery replacement or other checks to ensure reliable performance. It should be remembered that the cost of maintenance is often much less than the cost of replacement, so regular maintenance can significantly lower the long-term cost of ownership. Larger campuses may want to consider partnering with an outside resource like a locksmith or a security dealer for maintenance of door hardware and locks.

The most effective lockdown procedures include regular training for faculty, staff and students.

The Latest on Lockdowns

National standards for school lockdown procedures are beginning to emerge. However, the responsibility for developing a lockdown policy still lies with individual facility administrators. By design, a lockdown ensures that all internal and external doors and windows are locked or secured. Occupants inside the building(s) remain in their secured rooms and await an "all clear" announcement from emergency personnel.

The most effective lockdown procedures include regular training for faculty, staff and students. Teachers and staff members are often the initial responders to an emergency, yet few are trained properly in how to respond. They should have school maps and inventories of classroom emergency equipment and should conduct annual lockdown drills.

Effective emergency management plans rely on communication methods that distribute emergency instructions quickly and widely during a crisis. Public address systems, messaging via networked computers, electronic signage and other devices can alert everyone that an emergency lockdown must be performed because of a dangerous situation. The notification system(s) should alert all areas of the building, campus or district, including remote buildings and outside areas.

To implement a lockdown in the case of a hostile intruder, basic procedures should include:

- Lock all doors
- Close all windows and window treatments
- Remain low to the ground and away from windows and doors
- Turn off lights
- Move out of hallways and open spaces, if safe to do so
- Return indoors, if safe to do so
- Remain calm
- Await the "all clear" signal before releasing anyone from a room

When it comes to securing a school or building, there is no "one-size-fits-all" lockdown solution. The age of the facility, credential management platform and inherent protocols, and budget and long-term security strategy must be considered. The next step is to determine if a manual, remote/local, or centralized lockdown – or some combination thereof – best suits the facility.

Manual Lockdown

A manual lockdown relies upon an individual having the right key in hand and being at the opening. The speed of the lockdown is dependent on how fast an alert is communicated throughout the facility and how quickly the person can get to the door to lock it. Manual lockdown requires the greatest amount of staff accountability. However, it is also the most economical solution.

Remote/Local Lockdown

A standalone electronic lock solution provides instant local lockdown, which is activated with a remote fob. This solution relies on staff members to put the door into lockdown mode. Nonetheless, it is easier and faster to implement than a manual lockdown and is the most economical electronic solution.

Centralized Lockdown

This option requires only a single point of accountability. A lockdown is activated via a computer with access control software. It can be the fastest solution because one function simultaneously locks all openings on the network when a specific combination of access control software and hardware are in place. The organization can retrofit locks easily in existing structures since there is no need to hardwire each opening. It is typically the highest-cost solution.

Safe Schools Week

Safe Schools Week will be observed across the United States Oct. 19-25. While past years have emphasized bullying and other safety issues, this year would be a good time to use the week to raise awareness of physical security challenges and solutions in classrooms.

Back to TOC

April Dalton-Noblitt is director of vertical marketing for Allegion (www.allegion.com). She can be reached at april.dalton-noblitt@allegion.com.

Hackers and thieves are looking for the weakest link. Implementing simple and strategic security policies and procedures can protect you from 98 percent of the threats.

Target, eBay … and You?

Cybersecurity threats are real, even for small businesses

By **Hank Goldberg**,
Vice President
Secure Global Solutions

What does your business have in common with Target and eBay? Preferably, *not* the cybersecurity weaknesses that recently cost millions of dollars, exposed 100 million user records, and created lost consumer confidence that will last for years to come. But your business is just as vulnerable if you are not devoting time to the security task. As the *Symantec Internet Security Threat Report* noted in its review of 2013, "any business, no matter its size, was a potential target for attackers. This was not a fluke. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. In fact, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them."

"C" level executives (CEO, CFO, CTO) must put cybersecurity on their "to do" list. This article removes best practices as important first steps. If you are doing the basics, congratulations, you are in the top 20 percent. Extending security should follow into every part of the business,

from marketing to social media to product deployment.

Understand the Business Risk

The good news is that mistakes are preventable and vulnerabilities are correctable – or, at least, manageable with due diligence. Pay attention to the details of network security and create an action plan as the cornerstone of managing cybersecurity risk. Hackers and thieves are looking for the weakest link. Implementing simple and strategic security policies and procedures can protect you from 98 percent of the threats.

The starting point is knowledge about the data you hold and the risk it brings. Understand the data controls and eliminate unnecessary access. Blind trust is misplaced, and you must provide for audit and validation. Regular audits close vulnerabilities and eliminate malware. Do you audit financial statements? Of course. Validate insurance claims? Certainly. Every valuable corporate resource should be audited, and controls should be triple-checked to ensure proper asset utilization. Alarm and customer data is too precious to rely on processes only.

> Extending security should follow into every part of the business, from marketing to social media to product deployment.

Data Needs Protection

Guidance from professionals is needed to define the cybersecurity action plan. External experts who live in the gray world of data communications are available in every locale. Look for specialists in your field. Signaling, hosted solutions, credit card processing, HIPAA, DOD, and SEC compliance may all be considerations in your selection of an expert person or firm and may be included in a security audit. Diligent network scrubs and vulnerability scans are important defenses that help to keep a business off the casualty list.

Securing the personal information of customers must be a priority. In addition to credit card and billing data and demographic and contact information, passcodes, when used, must be considered. Since people reuse them, a passcode may provide a hacker access to bank or credit card accounts.

Create an Action Plan

Too often, the complexity of security seems overwhelming. A good place to start is with basic safeguards and vulnerability audits. Recognize that, in 2013, companies took an average of 229 days to detect network malware, according to the *Mandiant Threat Report*. Several affordable best practices should be implemented, including:

Create a protected perimeter

- Firewall – Protect the castle with a wall. Any network or device

that is not under your security control should be separated from your internal networks with firewalls. Purchasing equipment is a start, but make sure the firewall is updated on a continuous basis.

- Intrusion Detection Services (IDS) – Defend the perimeter with active monitoring of activity through the gates. Attacks can delay signals or compromise voice communications. IDS are available from companies that sell firewall services.
- VPN Access – Any internal data that passes outside the perimeter must be secured. Require secure credentials and encryption for all external users that are allowed inside. VPNs are simple and secure.

> The greatest risk comes from inside the organization.

Know your internal operating environment

- Conduct a network audit – The network design should be fully documented with IP addresses, device names, networks, communication connections and services. Any IT company should be able to help.
- Create a data map – Where is the credit card information, site data, passcode data, etc. stored? What users/applications have access to that data?
- Passwords – Develop a multi-level plan for secure access to internal equipment (i.e. servers,

routers, etc.). Also, plan for individual users accessing or changing any data.

- Remote offices and mobile users – PCs, mobile devices and branch offices are all part of the security landscape. Remote office connections should be secured outside the firewall if the devices and networks at the location are not under your security control. Develop standards for mobile devices that ensure that company data is secure.
- Desktops and servers – Purchase antivirus and antimalware for every workstation and server.

Improve defenses with active cybersecurity services

- Vulnerability assessments – All Fortune 500 companies use security audits as an anchor for ensuring quality delivery. Changes in devices or employees bring new risks to review. Assessing change and the impact on operations requires continuous vigilance.
  - *External vulnerability* – The first line of defense is the perimeter. Make it secure and conduct semi-annual audits. Large companies often conduct quarterly audits.
  - *Internal vulnerability* – The greatest risk comes from inside the organization. An audit can expose many problems with staff and systems. This is more expensive than an external vulnerability audit and should be done at least annually.
- Device monitoring – Bandwidth utilization and equipment performance measurements are great indicators of potential security problems. In addition, you may find unpatched equipment or users who are abusing access privileges.

Create (and practice) an Incident Response Plan

- Be prepared to act quickly – Once a breach is detected, you must move fast to minimize the damage. During the attack is not the time to figure out what to do. All shifts should be familiar with the response plan and know their roles and responsibilities, including such things as which firewalls to turn off and what cables to unplug. The protection of the automation systems under attack should be as quick and simple as possible.

Looking to the Future

The latest high-tech offerings come with greater risks of exposure and vulnerability through unprotected networks. New products and services must be assessed for risk. IP services increase the risks – even into our kitchens and automobiles – that these new devices create by opening other angles for hackers to attack. Symantec's 2014 *Internet Security Threat Report* describes this predicament: "Baby monitors, as well as security cameras

and routers, were famously hacked in 2013. Furthermore, security researchers demonstrated attacks against smart televisions, automobiles and medical equipment. This gives us a preview of the security challenge presented by the rapid adoption of the Internet of Things (IoT)."

The goal must be to provide *both* the most innovative products *and* the protection that customers deserve. There is no instant solution, nor does one size fit all. Put security into every product and business decision.

And consider putting the annual *Internet Security Threat Report* on your reading list. It is released each April and is well worth an hour of your time.

The goal must be to provide *both* the most innovative products *and* the protection that customers deserve. There is no instant solution, nor does one size fit all. Put security into every product and business decision.

Budget Considerations

The final key step is to commit to a *continuing* solution through an annual budget. Initial costs for documentation and professional security auditing and vulnerability studies create a baseline for future work. Information such as credit card or medical data will add to the basic security requirements. It is not unusual for companies to spend 0.5 percent of annual sales on business security, much more than even five years ago.

Maintaining a secure environment is like insurance: It's not something you want to spend money on, but it is something you cannot live without. A severe breach is expensive and potentially devastating. Find the time and resources to implement the above solutions, and you will save a substantial amount in the long run.

Conclusion

The world of cybersecurity was rocked in August by a mega-breach involving 4.5 billion stolen credentials from more than 400,000 websites. Cyber criminals collected data from those various sources, created unique identities, and then matched the data with other stolen information, such as bank accounts. The fallout from this event affects more than 1.2 billion individual identities around the world. It is likely that simple exploits were used against many unprotected sites and a lot of unprotected data.

The Internet of Things is a dangerous place. An ounce of prevention is critical. A pound of cure may be too little, too late.

Back to TOC

Hank Goldberg is vice president of Secure Global Solutions (www.secglobe.net). He can be reached at hank.goldberg@secglobe.net.

In spite of its advances and obvious value, PSIM needs to evolve significantly before it becomes truly aligned with its goals.

Broken Promises: The Current State of PSIM

Physical security information management solutions have so far fallen short of expectations, but next-generation systems could change that

By **David Daxenbichler**,
President & CEO
Network Harbor

Physical security information management (PSIM) software promised to unite multiple safety and security technologies into a common alerting, response and management framework. While much progress has been made in making this promise a reality, many PSIM systems fail to deliver the breadth of coverage, ease and consistency of use, and range of functionality necessary to meet the demands of an increasingly automated physical security industry.

This article explores where PSIM technology is today, why it remains an essential tool, and how it falls short of the ideal. It then outlines how PSIM must evolve into a unified security management platform, and what organizations should demand as these more universal applications of PSIM begin to appear on the market.

Introduction

PSIM software solutions came about in response to an obvious challenge. As physical security became increasingly driven by technology,

each type of system, from a wide range of vendors, required its own user interface. Video management systems required a different type of expertise than did intrusion alarms. Access control functioned completely differently than fire and smoke alarms. Product vendors, wishing to lock customers into their technology, used these closed systems to prevent competition.

The headaches for safety and security professionals from these fractured environments are far from trivial. Incompatible systems introduce time delays, as separate systems must be manually correlated to gain a full picture of what is happening. Staff must be trained on multiple systems, or additional staff must be hired. When organizations merge, either duplicate systems must be maintained, or staff trained in one must either be retrained in the other or let go.

The promise of one central platform, with a single user interface for all essential safety and security functions, carries obvious benefits:

- One system for staff to deploy, manage and operate
- All essential alerts, alarms, real-time and forensic information accessed from a centralized application
- Simple integration for new or upgraded capabilities
- The ability to connect disparate events to gain fuller, immediate insight into rapidly changing events
- Lower costs resulting from systems and subsystems integration and reduced training expenses

> Integrated security operations remain a work in progress, with potentially dangerous gaps in coverage, delays in response, and inappropriate levels of response.

But has PSIM lived up to its promise? In spite of its advances and obvious value, PSIM needs to evolve significantly before it becomes truly aligned with its goals. More technologies must be brought under its umbrella, covering products from a wider range of vendors, with more capabilities under active management. It also has to become something less – less complicated to use, as well as a smaller drain on limited financial, personnel and operational resources.

The Limitations of PSIM

On the surface, it appears that PSIM should be a runaway success. It addresses a significant problem by supporting a variety of products from a variety of vendors. Large systems integrators and end users have warmly embraced it. And, yet, overall sales have not been impressive. Why? The answers are as simple as they are frustrating.

First, very few PSIM systems work with everything an organization needs to manage the full breadth of its safety and security operations. Systems that

work with video surveillance, access control and intrusion alarms, but omit fire and smoke alarms or sound recognition or anything else, leave customers with incomplete coverage. Even worse, different PSIM systems do not necessarily support the same range of subsystems. This lack of consistency leaves customers with difficult decisions to make regarding what has to be left out of the centralized PSIM framework.

Many PSIM systems support only a small subset of the full capabilities of the subsystems they manage. These "missing" features must either be monitored separately or left out of regular operational management activities. Once again, the customer must decide what is most important and what cannot be centralized, given the current state of the technology.

The end result is frustration on the part of the purchaser – exactly the opposite of what PSIM is supposed to provide. Customers must still maintain separate systems. Integrated security operations remain a work in progress, with potentially dangerous gaps in coverage, delays in response, and inappropriate levels of response. Overall functionality is constrained by the limitations of the PSIM system itself, rather than the system providing comprehensive coverage for current and future needs.

In the end, critical resources must be assigned to uncovered or duplicate tasks. Training costs increase because of duplicated systems. And people and facilities are placed at unnecessary risk.

Next-Generation PSIM: Unified Security Management

The key to a next-generation PSIM system is to redefine the goal of PSIM, shifting away from what *can* be included under a single operational framework and toward what ***must*** be included for truly universal, fully unified security management. This new system – call it PSIM Plus – has to encompass all safety and security hardware and software solutions, as well as other elements, such as HVAC and facilities management, that can affect safety and security operations.

A PSIM Plus system has to be truly comprehensive, with direct integration of the following elements:

- Access control
- Identity management
- IP telephony
- Intercoms
- Tracking systems
- Sound recognition
- Facial recognition
- License plate recognition
- Unusual or unexpected behavior
- HVAC
- Fire/smoke
- Theft/intrusion
- Facilities management
- Video surveillance
- Visitor management
- Mass notification
- Geospatial integration management
- Workflow process management
- Enterprise management

There must be one single user interface for managing information from all of these systems, and it must be intuitive in its design so that anyone who is a properly trained safety or security professional can use it with minimal training.

Equally important, a PSIM Plus system must support the full application programming interface (API) capabilities of the underlying systems and subsystems. If a PSIM Plus system is to be a truly integrated information management solution, nothing should be left out, although customers should have the option of not using features that they do not want.

Finally, a PSIM Plus system must support an open systems approach, so that hardware and software from as many vendors as possible can be brought into its centralized environment. Open systems also simplify the challenges of mergers and acquisitions, since disparate products can all be managed through the PSIM Plus framework. The industry is already moving in this direction, but much work remains to be done in this area.

The Need to Work Together

One of the major hindrances for any safety and security technology, not just PSIM, is the ongoing conflict between vendors who must compete against each other for limited customer budgets and customers who want solutions that operate seamlessly with each other. The open systems movement is an attempt within the industry to ensure that hardware and software from multiple vendors integrates transparently.

These efforts need to continue and expand. Many, if not most, large-scale customers operate in heterogeneous environments and resist single-provider, walled-off solutions. In many cases, there is no alternative to purchasing products from multiple sources, since different vendors may have an industry specialization that is critical within a tightly focused, narrowly defined market. For example, federal and military requirements might be different from state and local government needs. Government agencies will have different priorities than multinational corporations. Energy production, with geographically dispersed facilities, has different needs than manufacturing, warehousing or

distribution organizations.

Vendors committed to open systems ensure that all of these pieces of the puzzle connect to create a more valuable whole. Once customers are confident that they have the flexibility and freedom to implement the features and functionality that are most important to them, they will also embrace the unified security management model. In short, working together while competing is in the safety and security technology industry's own best interest. The more it happens, the greater the opportunities will be for everyone.

How to Purchase a Next-Generation PSIM System

Enterprise organizations and government agencies seeking a next-generation PSIM system need to be clear about what they demand.

Comprehensiveness

As stated above, it begins with a system that delivers coverage for the widest possible range of systems and subsystems. It must have a single intuitive user interface. It must also provide the level of process standardization for assigning, resolving and archiving tasks that other enterprise-grade solutions routinely contain, including forensic capabilities for detailed reporting and process improvement.

Flexibility

A PSIM Plus system must adhere to open systems standards, built from the ground up to receive and present

data, video, sound clips, etc. from any subsystem's API. It must easily incorporate new types of technology easily and transparently. Little usability touches matter, too. For example, icons that scale as users zoom in and out from a map or diagram mean that critical information is never obscured from the operator's field of view.

Clear, uncluttered dashboard and display options help ensure that essential information can be read and interpreted quickly and accurately. Combined with detailed facility, location and object matching, operators gain the ability to understand not just that something has happened, but where and how other parts of the facility might be affected. Alerts and alarms must deliver the right information, when and where it is needed, whether to workstations within a security operations center or smartphones and tablets in the field, through direct access to the PSIM Plus software, or through email and text alerts.

Modularity

The system needs to provide a basic level of functionality, with the ability to easily add other capabilities later. That way, customers only have to purchase what they immediately need or can currently adopt, with future expansion in mind. In addition, software plug-ins can bring in critical data from other sources that might not normally be considered part of safety and security operations, but clearly provide additional value for protection of people and facilities. These include:

- Active directory
- Real-time system location
- Timed and linked events
- External web or cloud-hosted content
- Corporate IT biometric, two-factor and challenge logon
- Personnel records and ID management
- Visitor management
- Geographical information systems (GIS)
- Video wall management

Multiple Methods of Delivery/ Deployment

Some customers prefer a plug-and-play approach to technology. For these organizations, preconfigured servers or appliances are attractive. However, other entities prefer to install, configure and harden software on their own equipment. A PSIM Plus system should encompass both of these models. In addition, the system should be capable of operating in security operations centers, in addition to gathering data and delivering alerts across remote or geographically dispersed environments. The next-generation PSIM should also support software-as-a-service or cloud-based deployments, when such models prove practical for this market.

> Vendors committed to open systems ensure that all of these pieces of the puzzle connect to create a more valuable whole.

Workflow Management

It is no longer enough simply to capture and present data. The PSIM Plus system must also help users understand what to ***do*** with that data – quickly, transparently and efficiently. Workflow management is essential to this process and should cover the following:

- What to do when an alert/alarm event occurs
- Who should respond and what systems are affected
- How to determine that the situation has been resolved

These components must be automated, with full assignment, completion and task duration logging, as part of regular performance review and system improvement efforts. Preset templates can handle most basic applications, with drag-and-drop editing for modifying or creating new rule sets. As with the overall monitoring process, building rule sets should be intuitive and not require actual coding

skill, although that option should be available for more complex tasks.

Security

As with any enterprise-level, scalable solution, a PSIM Plus system must rely upon encrypted communications and robust storage protection for itself, its systems and its subsystems. Administrative rights, user permissions/authentications and user/group profiles should provide additional levels of segregation of duty, so that only authorized personnel have access to specific levels of information.

Conclusion

A PSIM system that does not provide universal coverage of all aspects of physical security automation is only a partial solution, at best. As powerful as the current PSIM products on the market may be, they all fall short of the ideal. Whether because of limited functionality from subsystem APIs, proprietary single-vendor strategies, or any of a wide range of other limitations, the idea of a *universal*, truly unified security management platform is just now starting to become a reality.

The key to creating the next-generation PSIM system is customer demand. The criteria for anyone choosing an integrated security management platform are simple:

- Use an open standards approach to work with as wide a range of hardware and software subsystems as possible.
- Provide full functionality for those subsystems' native APIs.
- Use a consistent user interface across the enterprise, so that safety and security professionals only have to learn one system, regardless of how many subsystems are providing data to the unified solution.
- Make the system simple to deploy and cost-effective to manage, with a modular approach that ensures customers can purchase only what they currently need.
- Demand that the system be available using a variety of delivery methods, with alerting and response capabilities driven by smartphone and tablet, as well as laptop and workstation.

The key to creating the next-generation PSIM system is customer demand.

Ensuring safety and security is increasingly a data-driven process. Next-generation PSIM is a critical part of making that process practical and efficient. Careful selection of the right solution for an organization will be the key differentiator in how fast and how well staff will be able to handle increasingly complex day-to-day protection demands. **Back to TOC**

David Daxenbichler is president and CEO of Network Harbor (www.networkharbor.com). He can be reached at d.dax@networkharbor.com.

It has become vital to our safety and security that we actively and continually assess who people are and whether or not they belong at a particular location at a specific moment in time. We have a responsibility to authenticate more than the individual.

Who Is Entering Your Facility?

Verifying identities is challenging; partnerships can help

By **Daniel Krantz**,
CEO
Real-Time Technology Group

Recently, tragic events have drawn attention to the challenge of truly knowing who people are, whether they belong inside a secured area, and if they've maintained compliance with access requirements that are designed to ensure safe and secure work environments.

As a co-founder of the Secure Worker Access Consortium (SWAC) – a community of contractors who support the construction, maintenance and operation of the World Trade Center and critical infrastructure in the New York area – I have had the honor and privilege of leading the technical development and operations of this unique public-private partnership. Our mission to understand who gains access to sensitive facilities and critical infrastructure has produced many valuable observations and lessons. This article will share some of the knowledge that we have gained as we have developed and improved the

Understanding the Insider Threat

When we ask, "Who accesses," what does that mean? The generic answer – "employees, contractors, vendors and visitors" – is easy. Unfortunately,

simply verifying that an individual was given an ID card has repeatedly proven ineffective and, in some cases, deadly.

Bad things rarely occur suddenly. Even when they do, the root cause can often be traced back to certain actions, or a lack of action. People do bad things, whether intentionally or not. It is our job as safety and security professionals to try and protect all who enter our facilities. One threat, in particular – the "insider threat" – is a serious vulnerability that creates opportunities for highly undesirable events, including workplace violence, sabotage and theft. The more we understand about an individual, the more effectively we can intervene before tragic events occur.

Developing a more comprehensive and effective identity profile requires a clear understanding of our current vulnerabilities. How do people hide personal information that would otherwise identify the threat they represent? Here are some of the vulnerabilities that we have identified, along with some of the risk mitigation techniques that can be employed.

One threat, in particular – the "insider threat" – is a serious vulnerability that creates opportunities for highly undesirable events, including workplace violence, sabotage and theft.

Personal Misrepresentation Empowers Insider Threats

"Personal misrepresentation" refers to common ways in which people conceal attributes regarding their identity that may disqualify them from gaining access to a facility. These attributes include, for example, presentation of fraudulent identity documents or false claims to employment, academic degrees or professional certifications.

It is very difficult to validate the authenticity of government-issued identity documents. Fraudulent documents are readily available, many of which are indistinguishable from the real ones without specialized equipment. Yet, these very documents commonly serve as the baseline for measuring an individual's identity and any related employment affiliations or educational achievements.

This places a burden on identity management program administrators to incorporate document authentication and identity verification processes in the enrollment process. Depending on the level of risk associated with a given program, different techniques can be utilized to meet this unique need. For example, at a basic level, an individual's pedigree information (full name, date of birth, Social Security number, foreign visitor or immigration data) must be confirmed as valid, with checks against deceased individual registries and

government watch lists. This is easily achievable via publicly-accessible databases at a reasonable cost.

As the risk at sensitive locations increases, so should our scrutiny of this critical identity information. If we cannot trust the personal identity verification process, how can we trust any additional screening or vetting that is conducted based on the subject's pedigree data? We simply cannot. Failing to properly authenticate an individual's identity presents a significant vulnerability to any security program. This vulnerability can easily be exploited to gain an inside advantage and, therefore, it must be addressed in the risk mitigation process.

Physical and Data Security

Ideally, we need to formalize how people register for participation in identity programs, using best practices for information collection, protection and authorized use. In fact, it is important to clearly understand and accept that with the collection of personal information comes the responsibility and duty to audit access to it and protect it from unauthorized exposure. This obligation begins with providing all participants with full disclosure regarding how personal data is used to verify other relevant security information. By presenting the required legal notices and collecting the relevant authorization forms at this early stage, program administrators can be assured that participants have knowingly provided consent for required investigations and have agreed to comply with the screening and vetting requirements of a given program. The ultimate goal is to find the appropriate balance between security requirements and privacy rights and expectations regarding the protection and limited use of personal information.

Document Authentication and Identity Verification

Secure locations that require individuals to present government-issued identification provide an excellent frontline opportunity to gain the trusted compliance of participating individuals and quickly validate the authenticity of identity claims. At trusted enrollment centers, documents presented can be technically analyzed for authenticity by verifying the embedded security features found in modern identity documents.

This critical step improves the integrity of any subsequent research regarding relevant personal attributes, such as verification of criminal background, employment history, certified skill sets or academic degrees. Similarly, an individual's identity information is commonly used to track other relevant personal attributes that have an impact on compliance with safety and security best practices.

More than Validating Names

Just because I am who I claim to be does not mean that I belong in a particular secured location at a given moment in time. Personal attributes such as past criminal behavior, emotional instability, civil litigation or extreme financial liabilities could all play a part in evaluating an individual's suitability for access.

Unfortunately, there isn't a one-size-fits-all identity profile. Security managers must evaluate their unique circumstances and implement safety and security procedures that suit the needs of broad-ranging risk profiles. For example, critical infrastructure protection programs generally rely upon the validation of an individual's identity, potentially disqualifying criminal offenses, and employment relationships with relevant organizations. Workplace safety programs may also incorporate safety or operations training in the compliance matrix. First responder and emergency management programs focus more on the various roles of emergency responders, how to ensure compliance with training requirements, and/or how to optimally deploy limited resources in response to natural disasters, hazardous incidents, and all

types of domestic and international terrorism.

Complicating matters is the dynamic nature of this type of information. People's lives change, and those changes can directly affect their ability to maintain compliance with criminal background standards, fitness evaluations, professional training and certification requirements, and employment policies. While an individual's identity rarely changes, and once validated can generally be trusted, these personal attributes must be continually monitored in order to maintain trust over an extended period of time. Re-evaluation periods are dependent on local policies and must be adjusted accordingly.

Perpetrators of undesirable events are often found to be repeat offenders, moving from one organization to another, leaving behind a recognizable and documented pattern of harmful behavior.

Performance Histories Provide Valuable Intelligence

Taking a deeper dive into an individual's performance history over time offers the opportunity to gain valuable intelligence. Given legal authorization during the enrollment process, identity management programs can facilitate the sharing of critical threat indicators among human resources, operations and security professionals.

These indicators may result from the documentation of incidents involving violation of policies, adverse screening reports or employment reviews, or inflammatory workplace incidents. Relevant risk factors identified in incident reports may provide cause for re-evaluation, further investigation, or even revocation of an individual's privileges. It is important to note that the value of incident reports may extend beyond a particular employment situation. Perpetrators of undesirable events are often found to be repeat offenders, moving from one organization to another, leaving behind a recognizable and documented pattern of harmful behavior. The challenge is to recognize those patterns and intervene early enough to prevent incidents that could result in large-scale public harm.

Monitoring of social media outlets has recently proven to be an effective tool in assessing the emotional stability and ideology of potentially threatening individuals. The right to review social media activity can be made a condition of employment and can be leveraged by appropriate ongoing screening and security initiatives.

As comprehensive identity profiles grow increasingly sensitive with the compilation of information provided by applicants, public data sources, human resources departments, employment

screeners, certification authorities, and operations supervisors, it is imperative that agreed-upon privacy constraints are maintained in the aggregation, analysis and use of personal data. Program administrators must utilize technology that audits and restricts access to information in accordance with program requirements and in support of privacy guarantees.

Programs Must Be Operational, Not Aspirational

Unfortunately, this type of critical information is almost always buried deep in back-office systems, inaccessible to operational personnel as access decisions are made. Or the input of data is so delayed that we are forced to be reactive to events, rather than proactively attempting to intervene. It is critical that we correct this underutilization of valuable and actionable intelligence.

It has become vital to our safety and security that we actively and continually assess who people are and whether or not they belong at a particular location at a specific moment in time. We have a responsibility to authenticate more than the individual. To better protect our transportation systems, key resources, health care facilities, academic institutions and places of public gathering, we must:

- Positively identify people
- Confirm their employment affiliations
- Screen relevant personal history
- Enable real-time sharing of identity information to validate compliance with safety and security policies and procedures

Partnerships Enable Efficient, Effective Programs

It is unrealistic to think that any one agency or company can efficiently and effectively manage identity programs for all of the diverse groups of people that may enter its facilities. Contractors, vendors and visitors each represent unique challenges outside of the tracking of regular employees. Further, internal tracking of employee information fails to provide valuable intelligence to other employers who may be susceptible to serial offenders.

> By working together to develop and maintain trusted communities, the overall efficiency and effectiveness of security efforts improves, with the cost of improvement distributed among participating organizations.

However, it is commonplace for labor groups and contractors to provide skilled workers in support of large organizations and regional sensitive facility owners and operators. These are largely shared and transient

workforces that build, maintain and operate our transportation systems, utilities, health care facilities, academic institutions, chemical and pharmaceutical plants and other sensitive facilities. Individual efforts to develop identity management programs can only result in a massive duplication of effort and, consequently, an unnecessarily increased risk of exposing sensitive personal data.

The creation of regional partnerships in the form of trusted communities that transcend traditional political, corporate and industry boundaries offers many benefits. Through the adoption of some basic standards and cooperative agreements, labor groups, contractors, vendors, human resources managers, certifying authorities, and security professionals can unite their efforts to ensure that the people who enter secure locations are appropriately skilled, known, and threat-free, in accordance with local requirements.

Benefits for All Participants

Individual participants will be relieved to know that paper copies of highly personal information no longer need to be stored in multiple, often unsecure, locations. Identity management technology offers the ability to securely collect individuals' personal information, manage their compliance with program requirements, and authenticate relevant information as required without compromising privacy rights. Advanced encryption protects sensitive data at all times, and permission-based, need-to-know sharing of this information only occurs in conjunction with comprehensive auditing to guarantee user accountability. In order to maintain the trust and support of community participants, it is imperative that information sharing be restricted to only those personal attributes that are relevant to the security task at hand.

Labor groups have the opportunity to highlight their value, promoting known members' qualifications, skill sets and performance records. Contractors can easily track the compliance of employees, knowing their efforts are in accordance with broadly accepted standards. Responding to diverse requirements at various work sites is an overwhelming burden. Labor can better meet industry needs with access to prequalified and certified workers who stand ready to support the safe and

secure construction, maintenance and operation of America's critical infrastructure and sensitive facilities.

Human resources directors can easily and efficiently verify an individual's compliance with regulatory requirements and internal policies without the duplication of effort that is common in larger organizations that manage multiple facilities. Smaller organizations benefit from access to low-cost, hosted and managed solutions for maintaining compliance with otherwise complex and burdensome requirements.

Certifying authorities can more easily ensure that our nation's workers are properly trained and maintain compliance with applicable continuing education requirements. In addition, the ability to selectively authorize access to training and professional certifications eliminates the administrative burden of repeatedly validating individuals' records.

Finally, safety and security directors gain critical insight into relevant personal attributes that demonstrate compliance with local security protocols. Plus, threat indicators generated by incident reports provide valuable intelligence to security guards stationed at access points. Relieved of the burden of trying to identify and qualify access rights for people entering their facilities, attention can be directed toward other security initiatives and challenges.

What Can We Expect from Regional Programs?

The benefits only multiply as programs extend throughout large organizations, industries and regions. But what tangible impact can we expect from operating these types of personnel assurance programs?

For starters, it is easy to accept that program participants will benefit from improved operational efficiency. Cooperative programs eliminate the burden on any single organization to invest in the development and maintenance of enrollment portals that securely collect participants' personal information. Once an individual has been processed for employment at an organization, subsequent employers need not spend the time and money associated with repeating the enrollment process. With the proper authorization, and at no additional cost, each subsequent employer can gain

access to an individual's information, including background screening, training records and other relevant personal attributes. Eliminating this duplication of effort among regional organizations has an immediate and positive impact on the efficiency of limited employment screening resources in each participating organization.

This efficiency contributes directly to the effectiveness of security operations. Personal data that is collected during the enrollment process, and the resulting identity profile that evolves as additional personal attributes are aggregated, deliver actionable intelligence that enhances the access control decision-making process at any single location. Extending this valuable information to otherwise disconnected entities (with proper authorization) enhances the effectiveness of local efforts to validate identity and trustworthiness prior to allowing access.

Sharing this vital security information throughout an industry or region improves the overall cooperative effort. With each participating organization contributing to the growth of a trusted community, the value of that community increases without attrition or loss. As individual members leave the employment of one entity, the value of their identity profiles extends to the next employer without additional cost. Because of the monumental task of managing identities for all employees, contractors, vendors and visitors, cooperation of this type is imperative for success. Further, once collaboration among organizations begins, their cooperative efforts tend to grow as valuable intelligence is exchanged and success stories are recognized.

The simple existence of trusted communities that are used to identify trusted resources and manage compliance with security procedures helps reduce the risk of unknown offenders entering sensitive locations. Published criteria and well-managed screening services tend to work in a self-cleansing manner, pushing undesirable individuals away from secured facilities toward locations without such stringent requirements. This "path of least resistance" methodology is commonly used by perpetrators to identify "soft targets." The broader a community grows, the more risk is reduced through better coverage of regional vulnerabilities.

By working together to develop and maintain trusted communities, the overall efficiency and effectiveness of security efforts improves, with the cost of improvement distributed among participating organizations. Competition has its place when it comes to who provides the best commercial product or service, or who has the best company softball team. But when it comes to the safety and security of our sensitive facilities and public landmarks, we absolutely must begin to work together.

Back to TOC

Daniel Krantz is CEO of Real-Time Technology Group (www.realtimetg.com) and co-founder of the Secure Worker Access Consortium (www.secureworker.com). He can be reached at dkrantz@realtimetg.com.

A web-based solution can help organizations implement a business continuity plan that reduces risks, controls costs and ensures the safety and security of personnel and property.

Enhancing Continuity Planning Through Improved Security

Web-based systems can tie everything together

By **Kim Rahfaldt**,
Public Relations Manager
AMAG Technology

Large organizations must manage a myriad of building risks and functions to operate a secure and compliant business. They have to be concerned with credential authentication, visitor management, emergency preparedness, risk and vulnerability assessments, and incident management, among other things. To manage these processes, organizations often deploy disparate technologies and systems, each equipped with their own data mining and reporting procedures.

As organizations acquire businesses, they absorb existing security solutions, many of which have reached legacy status. How do they effectively manage separate security systems? How do they conduct business with minimal disruption? Do they need to rip out old systems, or is a retrofit system a viable solution?

To address these risks, many large corporations with multiple (BCP). BCP describes the processes and procedures an organization implements to ensure that critical functions can continue during and

after a disaster. To manage BCP, these multi-site organizations need a total solution that cohesively secures the organization, pulls data and shares data. If running multiple security systems, they must find a way to operate them while consolidating to one system.

A web-based solution can help organizations implement a BCP that reduces risks, controls costs and ensures the safety and security of personnel and property. It can also help organizations avoid corporate liability issues, industry fines and compliance problems, while managing multiple security systems.

Integrating visitor management into a total web-based solution saves time, and sharing critical information creates a safer environment and solves many challenges.

Data Management

Organizations with multiple locations have data and information located everywhere. It can be in a spreadsheet on a branch manager's desktop or in a database like IBM Notes. Any data held in an offline format can quickly become stale. It is difficult to share, and updates are hard to manage. A web-based solution provides a way to consolidate and standardize data, while enabling hundreds of people throughout an organization to access it and pull reports. The automation saves time and allows employees to provide an enhanced level of service to customers, rather than spending hours searching for data and consolidating it into a report.

Emergency Preparedness Challenges and Solutions

Emergency preparedness is only one part of emergency planning, which is a subset of the larger BCP. Large institutions must ensure that all people, facilities and assets are secure and fully equipped to handle emergency situations. Often they do not have a comprehensive emergency preparedness program to coordinate fire evacuation and life safety efforts in administrative facilities. These gaps expose organizations to legal and regulatory risks, and employees and third-party tenants to unsafe working conditions.

Organizations may have emergency preparedness programs in place, but each location may be managing the program differently and not sharing the information. A web-based solution can dynamically manage emergency action plans and audit all tasks related to emergency preparedness training, drilling and plan maintenance.

Emergency preparedness programs can be set up fairly quickly by distributing responsibilities among team members. Each location completes a site survey, selects and

trains a response team, performs scheduled drills, and maintains plans to ensure ongoing compliance. A central database manages all emergency response teams and provides reporting capabilities for audit purposes. The software updates and publishes team plans, providing all vendors and employees seamless access to floor plans, evacuation routes, important documents and emergency response teams. The software manages by exception, identifying discrepancies by interfacing with the human resources database, and automatically notifies team members of overdue drills, training or certification renewals.

The Occupational Safety and Health Administration (OSHA) has stated that, "Employers are responsible for providing a safe and healthy workplace for their employees." Web-based solutions can help institutions maintain compliance with OSHA requirements, as well as many international, state and local fire and emergency codes.

Visitor Management

Managing visitors in a large organization can be a complex challenge that results in major frustration for everyone. Many companies use a paper sign-in procedure with no pre-authorization required. Other possible pain points include an inability to report on visitors, no integration with a card access system, which creates a security loophole, no automated "Do Not Admit" list, an inconvenient and slow process for guests, and no way to process or track visitors without a security officer.

> It is difficult to collect data without the right tools.

Integrating visitor management into a total web-based solution saves time, and sharing critical information creates a safer environment and solves

many challenges. With a web-based system, employees simply log into the software and pre-authorize their visitors. The visitor's ID is validated, compared to the visitor list, and a photo is taken. Barcode readers on turnstiles, doors and elevators can integrate with the access control system, allowing a visitor access to multiple areas in a facility as needed.

Risk and Vulnerability Assessments

As organizations implement their BCPs, they must assess and mitigate risks across their locations. However, they often do not have a central system to store site security data and must, instead, rely on information that lives on a spreadsheet or in someone's head. It is difficult to collect data without the right tools.

Additional gaps in security can occur when there is no standardized way to assign risk levels to locations, no ability to weigh asset risk against mitigation, no way to analyze trends and no ability to determine what is important to an organization.

With a web-based solution, all site information can be placed in a central database for all to access. The information is populated through surveys or database links, and each site can be assigned a data owner to collect information.

Incident Management

Managing incidents across a large organization requires an interactive event management and tracking tool used by several people throughout the company. Incidents must be recorded quickly, automated notifications must be sent, and a workflow must be created to handle the incident. A web-based solution can enhance security by producing automated reports that can spot trends and analytics information that can be used to prevent recurrence.

Credential Authentication and Retrofit Solutions

Companies with aging or legacy security systems face many challenges. Often, they are managing disparate access control systems and databases, have decentralized access management, use a manual access request process, use a paper and/or email-based audit system, or are married to one legacy access control platform. A web-based overlay solution establishes a single user interface to manage multiple access control systems, moves the system to a distributed, centralized or hybrid access assignment model, implements an online access request system with workflow approval, automatically audits employees' access rights, and can gradually migrate the company to a new access system as budget allows.

A retrofit solution provides an inexpensive upgrade that allows organizations to use their existing cards, readers, enclosures and infrastructure.

In large organizations, different groups are established with one person in charge of access rights. For example, one person would oversee access in each branch office of a bank. The access control representative assigns access rights and manages the system, performing all functions from a single screen with the ability to assign and remove access, activate and deactivate access cards, transfer audit responsibility, and add personal attributes to the system.

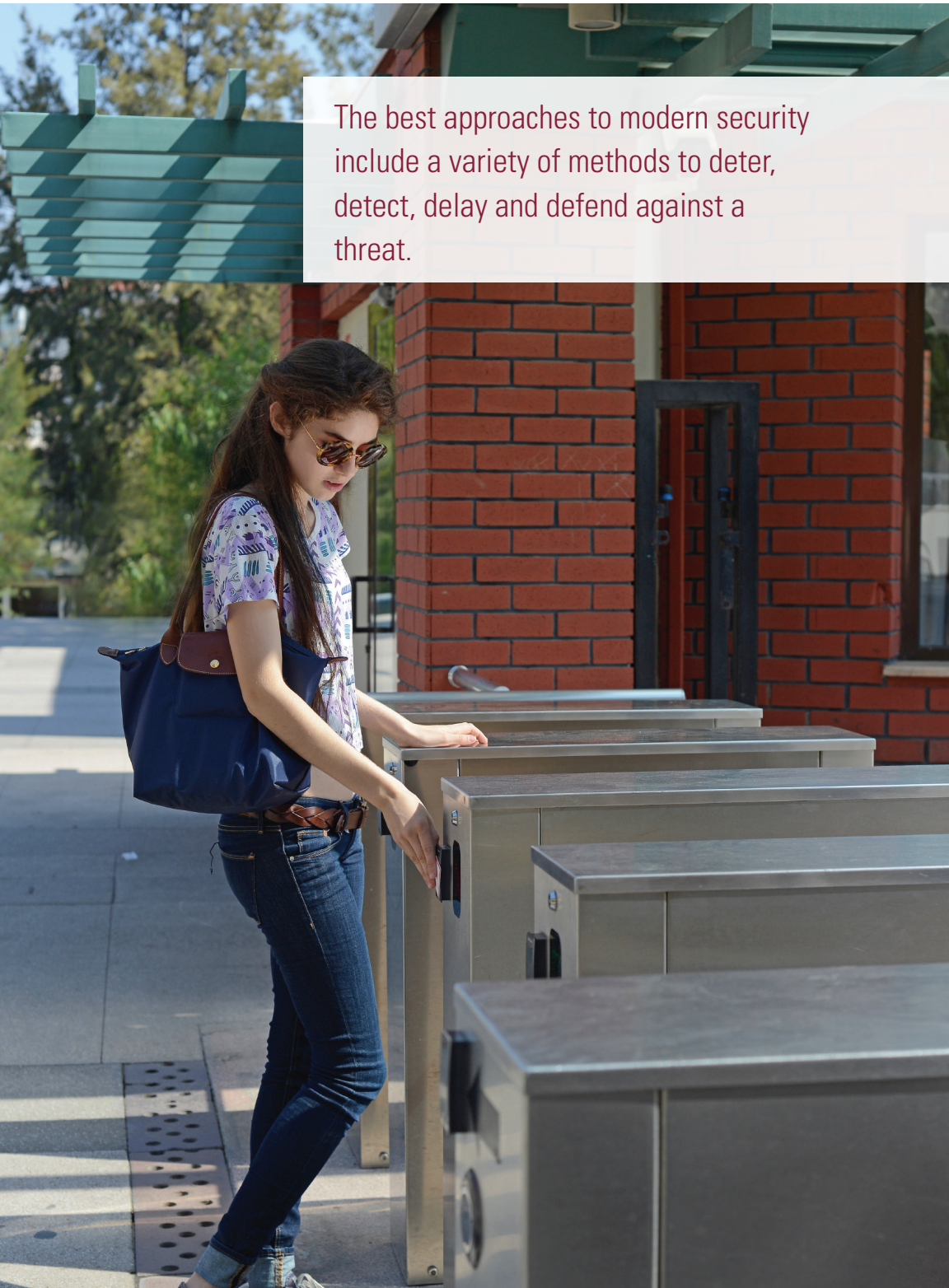
Organizations with older systems may want to consider a retrofit solution that upgrades a building's security technology to a state-of-the-art platform. A web-based system can bridge the gap by providing a single interface for multiple users while the retrofit system is being installed.

A retrofit solution provides an inexpensive upgrade that allows organizations to use their existing cards, readers, enclosures and infrastructure. It can be used side-by-side with other security systems when a web-based system is also used. Companies can share data across departments, integrate disparate, legacy security systems, and manage access using one dashboard. As companies migrate to the new access control system, the web-based solution provides an easy-to-use platform – and a total solution.

A web-based system can act as an overlay and provide detailed reports so management can make better informed decisions about security and procedures. Reports on these activities can offer real-time information, increase security and help organizations stay compliant with regulations, which are all components of a BCP.

The all-inclusive, easy-to-use web-based software allows end users to stretch their dollar and maximize their product to mitigate risk and improve overall security. **Back to TOC**

Kim Rahfaldt is public relations manager for AMAG Technology (www.amag.com). She can be reached at kim.rahfaldt@amag.com.



The best approaches to modern security include a variety of methods to deter, detect, delay and defend against a threat.

Enabling Safe Learning Environments

Securing schools demands a layered approach

By **Neil Lakomiak**
Director
UL

Most people agree that maintaining a safe environment is essential to learning. Safety is second only to food, water and air in Maslow's Hierarchy of Needs, and it is required to realize higher order needs like achievement, confidence, creativity and problem solving.

Recently, tragic violence in our nation's schools has garnered much attention and placed a new level of urgency on safety. Some funding to improve school safety has been made available at the federal level, and various grants are being awarded to ensure schools have an emergency management plan, that students get treatment for mental health issues, and that a safe and positive educational environment is promoted. This has led to more school districts installing more locked doors, more visitor check-ins and more surveillance equipment.

While security is top of mind upgrades. Achieving the goal of a safe school incorporates many facets, including things like access control, intrusion detection, fire protection, indoor air quality and emergency

communication. How should we manage these areas and focus on prevention? How can codes, standards and technology, in conjunction with an overall safety strategy, help promote the safer learning environments we seek?

How can we create a competitive environment for school security, much like there is competition for LEED recognition?

Model Codes for School Security

Development and enforcement of fire and building codes has been a major factor in keeping our children safe in school. Most schools built since the late 1970s have been required to have sprinkler and fire/smoke alarm systems. Fire protection, egress, emergency communication and construction standards have done much to mitigate the loss of life and property.

Progress has recently been made in developing general installation standards and recommended practices for security systems, in some instances, specifically for schools. While these efforts are a move in the right direction, what is missing is an overarching model code, like the codes in place for fire safety (ICC International Fire Code/NFPA 1) and building construction (ICC International Building Code/NFPA 5000).

Effort has also been expended to promote more efficient buildings – including schools – through green building codes, with an emphasis on acquiring coveted Leadership in Energy & Environmental Design (LEED) credits and ratings. How do we get people equally excited about the security of our schools and, ultimately, the safety of our children? How can we create a competitive environment for school security, much like there is competition for LEED recognition? Such excitement could start with a model code for security in schools.

Vulnerability Assessments

Normally, the first step in developing a security strategy is to conduct a

vulnerability assessment. A thorough assessment is essential for identifying and understanding security risks and their relative magnitude. The end goal of any security strategy is to protect an asset, and, given the uniqueness of each school, there will not be a one-size-fits-all solution. For schools, the students, faculty, staff and visitors are the most important assets. A proper vulnerability assessment can determine what an adversary might exploit at a given location. For new schools, a vulnerability assessment means that security can be part of the school design process from the beginning.

> When considering the many potential uses of school facilities, access control technology offers a means to effectively and efficiently strike a balance between ensuring safety and enabling normal operations.

Egress is another major factor to consider. While there is an obvious focus on keeping the "bad guys" out by having windows and ingress points limited and secure, building occupants need to be able to escape in the event of a fire. Further, law enforcement and fire fighters must have access to a building during an emergency.

Fitting the Pieces Together

In short, vulnerability assessments serve as an input to a security strategy, where a mix of people, processes and technology are optimized to achieve the overall security goal. When assessments are combined with a

model code for security and a security strategy, these three pieces can be used to develop long-range plans to upgrade school safety. These plans, in turn, give schools the power to be proactive about security and may improve their chances for receiving grants or other funding.

In addition to assisting in the development of a long-range plan, building a strategy upon a vulnerability assessment, model codes and standards can also help to improve efficiencies in how money is spent on security. Codes and standards provide an objective means by which to identify the appropriate mix of people, processes and technologies needed to achieve the desired levels of security.

Technology Tools for Safer Learning Environments

Access Control

Access control is one of the most effective technologies in limiting entry to authorized visitors who have a stated purpose for being inside a school. It permits efficient entry of authorized persons into a secure area and keeps out those who have not been vetted.

There is a vast array of access control solutions, hardware and software that can be deployed in a way that prevents disruption of the normal course of business at a school. To identify an optimal solution, the following factors should be addressed:

- Students entering the school outside of regular operating hours for extracurricular activities
- Student movement between buildings as class schedules dictate
- Parents transporting children or picking up or dropping off school-related materials
- Vendors delivering materials and supplies
- Public use of school facilities for community activities

When considering the many potential uses of school facilities, access control technology offers a means to effectively and efficiently strike a balance between ensuring safety and enabling normal operations.

Dynamic scheduling, another feature of access control systems, provides options to permit or deny

access before or after certain times of day. However, while the primary function of an access control system is to prevent unauthorized access, a proper interface with a fire alarm system is imperative to permit orderly egress in the event of a fire. NFPA 101, Life Safety Code, is the primary document that addresses this requirement.

While life safety may be the single most important priority for access control systems, the technology can also be an effective tool for protecting property. As many schools invest tens of thousands of dollars in technology such as computers, tablets and other devices, there is a growing need to secure these assets. The shrinking size of computer devices has made them a prime target for theft, as they have become much easier to conceal. Access control systems can effectively protect these devices, in addition to everyone coming in and going out of the school.

> It is important to keep in mind that adding more cameras to a facility does not necessarily equate to more security.

Visitor Management Systems

Visitor management systems are another effective way to control who enters a school. Many permit regular guests, like parents, to register, upload a picture and state the purpose for visiting. Some also incorporate kiosks for self-service, allowing administrative personnel to focus on other activities. Other systems even include a background check to vet

new or currently enrolled visitors on an ongoing basis. As these systems evolve, they are encompassing access control, visitor management, time and attendance and other functions into a single architecture.

Video

Video is becoming a staple technology for safer schools. It directly supports the main principles of security: deter, detect, delay and defend. Schools can use video, for example, to monitor a parking lot or the perimeter of school grounds. Early detection of a potential intruder gives school authorities time to take action and stop that person from gaining entry. Video also acts as an effective deterrent because, if people who do not belong there know they are being watched and recorded, they may be less likely to try to enter the facility.

A potential, and unintended, consequence of video technology use is that it may give the end user a false sense of security. It is important to keep in mind that adding more cameras to a facility does not necessarily equate to more security. In order to measure effectiveness, one must gauge how the cameras are used, where they are located, and whether or not someone is continually monitoring them.

Choosing the right video equipment can be daunting, considering the many varieties of products, features and functionalities that are available. This has created a strong demand for performance standards for video equipment, which provide a way for end users, integrators, specifiers and procurement professionals to objectively compare one product to another and make better price-versus-performance decisions. With this information, schools can be smarter about how best to use their scarce security dollars.

Video Analytics Software

Video analytics software has also proven useful. Depending on the size of a campus, it may not be practical to have personnel constantly monitoring camera feeds. Video analytics can be employed to detect specific scenarios and generate an alarm or alert condition. One example could simply be the detection of someone or something in a predefined area, like a locked rear entrance, where there should not be an object appearing.

The pace of innovation with video technology is impressive. Technology is now available for remote and mobile monitoring of live video feeds, which enables law enforcement and other authorities to see inside a school while en route to an unfolding incident. Because it enhances situational awareness, video can help determine how to organize and stage first responders, both in advance of and upon arrival.

Physical Security

Physical security technologies to consider include products like door hardware and locks. These range from simple mechanical options to sophisticated electro-mechanical devices. A popular approach is to use

electro-mechanical locking devices in conjunction with an access control system. In the event of an emergency, an entire school can be locked down in a matter of seconds.

Selecting the right hardware options is essential. Keeping a door locked from the outside, while still enabling safe egress from occupants inside a classroom is essential. Newer locking arrangements on the market are designed to eliminate the need for a teacher to lock the door from the outside. The latest technologies allow locking and unlocking from a central location.

Creating an Enhanced, More Secure Future

Violence in our nation's schools has rightly caused many to join the effort to find new and better ways to enhance safety and security. And, as discussed, a few ways to support this cause are by developing model codes and standards for school security and by leveraging a variety of technologies, whether they are tried and true or are on the cutting edge of innovation. We can also become more active in creating strategies and long-range plans that support the entire security ecosystem. Model codes and standards can help to enable more efficient use of scarce resources by providing objective requirements for securing schools.

The best approaches to modern security include a variety of methods to deter, detect, delay and defend against a threat. By leaning on industry experts, evaluating best practices, and weaving technological solutions together, we can promote safer learning environments and enable students, teachers and staff to focus on education. **Back to TOC**

Neil Lakomiak is director of business development and innovation for building and life safety technologies at UL (www.industries.ul.com/life-safety-and-security). He can be reached at neil.lakomiak@ul.com.

The car bomb represents a relatively easily obtained semi-strategic weapon that, under certain circumstances, is comparable to an airstrike in its ability to obliterate high-profile public targets, while terrifying a country's population.

From Horse-Drawn Wagon to Moving Truck

Nearly a century after the first VBIED was detonated in the U. S., what can be done to mitigate the risk of car bombs?

By **Laurie Aaron**
Executive Vice President
Building Intelligence

The themes of the story are well known. A militant who opposed the United States government decided to launch a mass-casualty strike in Manhattan to avenge the capture of his colleagues.

He filled a vehicle with explosives, parked in a heavily traveled spot, exited, and walked away.

This, though, was in September 1920, the vehicle was a horse-drawn wagon, and the attacker was Mario Buda, who was angered by the indictment two days earlier of anarchists Sacco and Vanzetti for a murder-robbery in Braintree, Mass., that April.

"The horse and wagon were blown to bits," Paul Avrich wrote in *The Anarchist Background*. "Glass showered down from office windows, and awnings twelve stories above the street burst into flames. People fled in terror as a great cloud of dust enveloped the area. … Scores of bodies littered the and wounded 134. Although it would not be known as such for many more years, this was the first vehicle-borne improved explosive device (VBIED) in U.S. history.

Now, nearly a century later, the car bomb represents a relatively easily obtained semi-strategic weapon that, under certain circumstances, is comparable to an airstrike in its ability to obliterate high-profile public targets, while terrifying a country's population. In terrorism's "modern era," the car bomb has been used multiple times, sometimes producing devastating effects – 168 deaths in the Murrah Building in Oklahoma City in 1995 – and sometimes ending without injuries or damage, as in the failed attempt to bomb Times Square in 2010.

Another VBIED attack in Manhattan, this one at the World Trade Center in 1993, provides a useful case study.

World Trade Center Bombing

The Sept. 11, 2001, terrorist attack that brought down both buildings of New York's World Trade Center was actually the second time that al Qaeda targeted the twin towers. The first was on Feb. 26, 1993, when a moving truck loaded with explosives was detonated in the parking garage below the North Tower in an attempt to collapse it into the South Tower. Both buildings remained standing, but six people were killed and more than 1,000 were injured in the blast.

In March 1994, four Islamic militants were tried in connection with the bombing and were convicted of charges including conspiracy, explosive destruction of property and interstate transportation of explosives. In November 1997, two more men were convicted, including Ramzi Yousef, the mastermind behind the bombings.

Bombing victims sued the Port Authority of New York and New Jersey, owner of the World Trade Center, for damages. In 2006, a New York jury determined that the agency was 68 percent responsible for the bombing, a decision that was upheld by an appeals court in 2008. In its ruling, the appeals

1993 World Trade Center Bombing: A Personal Account

Among the injured in the 1993 World Trade Center bombing was Scott Alswang, who was, at the time, a member of President Clinton's Secret Service team. Alswang later testified against bombing mastermind Ramzi Yousef in federal court.

Alswang described the scene in a July 2014 interview.

It was a snowy, overcast day in February. I was in the Protective Intelligence squad, investigating threats that had been transmitted regarding our "protects," that is, the president, vice president, etc. Myself and my colleague, who had recently retired from Secret Service, but was appointed by Governor Florio of New Jersey as the waterfront commissioner, drove together to pick up a third colleague assigned to our detail at her office. The three of us then drove together to One Police Plaza on a report of a box delivered and addressed to the president of the United States.

It was a false alarm. Rather than a bomb or chemical threat, the box actually contained human feces so we referred the case to another field office and left Police HQ. This was the start of what would prove to be the craziest day of my life.

After a morning of meetings ranging from the NYPD bizarre package investigation to the FBI for intel on a possible threat to the prime minister of Bosnia, we drove to our office at One World Trade Center and pulled into the B2 parking level, where the fleet of over 300 federal vehicles – black cars, armored limos, surveillance vehicles etc. – were housed. As a matter of habit, I kept my keys with me, whereas most cars were left with keys in them and were double parked due to lack of spaces. I dropped my colleagues in the lot and proceeded to find a space where I could park and take my keys.

As I backed my "G ride" into a space and put the car in park, the bomb went off. The windows of my car imploded, I was hurled to the passenger side floor, my glasses blown off my face. Glass embedded in the left side of my neck, cheek and forehead.

I did not know what had hit me. I crawled out of the car and hit the ground. It was pitch black and smoky and all I heard was car alarms, electric wires arcing and water pipes exploding as water flooded the ground.

My colleagues had been thrust under my car. I was yelling for them. They were alive. One had glass in both his eyes and could not see. The female colleague had a dress on. She was blown out of her heels. Her legs were cut and bleeding. As I helped them to their feet, we somehow made it to the concourse where there was nothing but mayhem.

I badged my way into a Chemical Bank to call the field office. Once we hit clean air, we all started vomiting. We hailed a cab who took us to the hospital. We had survived.

court judges cited the "extreme nature of defendant's negligence," and stated that, "the evidence overwhelmingly supported the view that the conscientious performance of defendant's duty reasonably to secure its premises would have prevented the harm."

In 2011, however, the New York Court of Appeals, in a 4-3 decision, ruled that the Port Authority could not be held liable for the bombing because it had engaged in "the type of informed, policy-based decision-making that entitles a governmental agency to immunity."

"Governmental entities cannot be expected to be absolute, infallible guarantors of public safety, but in order to encourage them to engage in the affirmative conduct of diligently investigating security vulnerabilities and implementing appropriate safeguards, they must be provided with the latitude to render those critical decisions without threat of legal repercussion," the majority opinion asserted.

> While governmental immunity saved the Port Authority from being held liable for the bombing, private sector building owners would not, obviously, be able to present the same defense.

The dissenting opinion stated that the rulings of the lower courts should be upheld "because the Port Authority's failure to implement discrete and basic security measures in the public parking area of the commercial building complex arose from the exercise of its proprietary – rather than

governmental – obligations. Treating the Port Authority as a private landlord, there was sufficient evidence at trial to support the jury's finding of liability and its apportionment of fault."

While governmental immunity saved the Port Authority from being held liable for the bombing, private sector building owners would not, obviously, be able to present the same defense.

Countermeasures

Even terrorists with minimal resources and little technical knowledge can use car bombs to cause massive destruction. Building owners are morally and legally responsible for implementing reasonable measures to protect their occupants. Fortunately, many things can be done to secure a building, and the publication *Protecting Buildings from Bomb Damage* from the National Research Council (available at www.nap.edu) provides excellent guidelines, some of which are detailed below.

The shockwave from a bomb blast is what causes much of the damage, and the power of this shockwave decreases proportional to the *square* of the distance. So the farther away a vehicle is from a building, the less damage it can cause to that building. Maximizing standoff distance, then, is the most effective and efficient approach to protection. The greater the standoff, the less hardening a building needs.

Even terrorists with minimal resources and little technical knowledge can use car bombs to cause massive destruction.

Perimeter

- Reduce vehicular approach speed by adding bumps and curves in the road. Control vehicular access with vehicle barriers, traps or hydraulic barricades.
- Use barriers, such as courtyards, plazas, landscaping, perimeter bollards or planters, fountains, reflecting ponds, and other features to ensure that a vehicle armed with a bomb would not be able to drive up next to the building and park.
- Maintain a clear zone between surface parking and the building (100 feet or more, if possible), and use barriers, planters or knee walls to protect the building from ramming.
- Identify all vehicles prior to entry and, if necessary, search vehicles that are allowed to park in or beneath the building. In extreme cases, parking under the building should be severely restricted or banned. Even then, procedures for identifying and inspecting the vehicles that do park there must be strictly applied.
- Keep public parking away from critical building systems, backup generators and gas meters.

- Identify all vehicles and drivers, even in public parking areas, if those areas are co-located with the building. This serves as a deterrent as much as a forensics tool.
- Improve lighting as appropriate for the area and in accordance with local ordinances.
- Increase site surveillance and monitoring capabilities and/or patrols.
- Use CCTV surveillance and license plate recognition solutions to monitor and record vehicle activity.

Building Exterior and Grounds

- Apply blast film to windows. This may be expensive, but it can save lives, prevent injuries and protect both equipment and documents in the event of a bomb blast.
- Secure and alarm windows and emergency egress doors that are accessible from the ground level. Also, secure the building from accessible roof levels and setbacks.
- Check the location and design of air intake grilles to address risks related to smoke and noxious gases.
- Keep loading dock doors closed. Where this is not practical, control access to the loading dock area, allowing only scheduled, identified vehicles to enter. Also, control access from the dock area to freight elevators, fire stairs and the building interior.
- Locate garbage skips and compactors within the building perimeter or, if outside, well away from the exterior walls.

Maximizing standoff distance is the most effective and efficient approach to protection.

Building Entry

- Have a separate entrance for employees with valid credentials.
- Process employees with credentials automatically using credential-reading systems, while those without building or corporate credentials must get their identity and purpose for being in the building validated before access is permitted.
- Allow only scheduled visitors to go beyond the lobby.
- Control and screen all deliveries. Consider a messenger drop-off center with a separate entry.
- Use internally cleared and uniformed personnel to document and deliver packages. Employees receiving lunch deliveries that require payment should pay for and accept the deliveries at ground level.
- Use airport-type screening (walk-through metal detectors and package x-ray systems)

for all seeking access to the building interior. In very high-security environments, use explosives-detection equipment for bags and people.

Building Interior

- Develop layers of security and place assets that are at high risk within the innermost layers. For example, secure each floor at the elevator lobby and – fire codes permitting – fire stair doors, and further secure sensitive operations within the floor.
- Locate building occupants away from portions of the building with direct street frontage. Use such areas for non-vital equipment or storage.
- Identify and secure assets that might be high-profile targets or that are most important to business operations. Such assets might include executives, managers, human resources personnel, receptionists, data centers, and voice and data cabling and equipment.
- Remember to account for rooftop assets such as wireless transmission equipment and emergency generators.
- Locate shipping and receiving areas in remote parts of the facility, and develop secure processes and access management for the "back door," as well as the front.

Conclusion

Whether in a developing nation or the United States, the threat of terrorism, in general, and car bombs, in particular, is real. Security strategies will change depending on the building and the assets within, but one thing that never changes is the responsibility of those tasked with security to assess and address risks honestly and without indecision. **Back to TOC**

Laurie Aaron is executive vice president and chief marketing officer for Building Intelligence (www.buildingintelligence.com). She can be reached at laaron@buildingintelligence.com.

securityindustry.org/techinsights

Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
301.804.4700