DomPrep Journal

Subscribe

Volume 18, Issue 12 December 2022

LEADERSHIP DEVELOPMENT SYMPOSIUM

JAN 9–11, 2023

JOIN US IN JANUARY

- 2-1/2 day annual symposium will be held at the Dallas Frisco Embassy Suites Convention Center
- No Admission Fee for Texas resident attendees
- $150 for out-of-state attendees

LEADERSHIP ESSENTIALS

The TEEX Leadership Development Symposium brings together some of the industry's most influential speakers to address leadership and management challenges faced by today's community leaders and emergency responders. You will discover insights and tools that will empower continual growth as a leader and manager in all life's areas.

REGISTER and Learn More

NEWSLETTER

Receive the most current event information by subscribing to our monthly newsletter.

TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

Questions?
979-321-6215

Leadership.Symposium@teex.tamu

TEEX.org/LeadershipSymposium

Business Office
313 E Anderson Lane
Suite 300
Austin, Texas 78752
www.DomesticPreparedness.com

Staff
MacGregor Stephenson
Publisher
macgregor.stephenson@tdem.texas.gov

Catherine (Cathy) Feinman
Editor
cfeinman@domprep.com

David "Randy" Vivian
Business Outreach
randy.vivian@tdem.texas.gov

Bonnie Weidler
Publications Liaison
bonnie.weidler@tdem.texas.gov

Martin Masiuk
Founder & Publisher-Emeritus
mmasiuk@domprep.com

Advertisers in This Issue:
TEEX Leadership Symposium

Domestic Preparedness Journal is electronically delivered by the Texas Division of Emergency Management, 313 E Anderson Lane Suite 300, Austin, Texas 78752 USA; email: subscriber@domprep.com.

Featured in This Issue

Building Strength in Workforce and Structure
By Catherine L. Feinman 4

The Importance of Strong Leadership for a Unique Discipline
By David Fogerson 5

Maintaining a Strong Volunteer Force
By Kristina L. Hamilton 10

Implementing "Stop the Bleed" for Future K-12 Educators
By Will Brewer, Peggy Bergeron, and Wayne Bergeron 13

Applying Environmental Design to Prevent Active Shooters
By Rodney Andreasen 18

Value of Enterprise Data Management in Emergency Management
By Anne Marie Smith 22

How Technology Systems Impact Critical Infrastructure
By Nathan DiPillo & Paul Galyen 25

Pictured on the Cover: Source: ©iStock/Panuwat Dangsungnoen

Building Strength in Workforce and Structure

By Catherine L. Feinman

The success of an emergency response is often based on the knowledge and abilities of the people in place to manage the situation and implement action plans and procedures. Each person plays a critical role, from top leadership to frontline workers. Leadership styles vary, but effective leaders build relationships and bridge communication gaps to motivate teams that begin long before they arrive at ground zero. In addition, good leadership strengthens the workforce and improves decision-making in areas like fortifying the physical environment, thus creating more resilient communities.

However, it is essential to note that *leadership* is not a proprietary term reserved only for incident commanders, and no matter what someone's rank, the learning process should never end. For example, volunteer coordinators and emergency response trainers must recruit, educate, and train future responders. Preparing people to run toward danger when others run away requires a leader who inspires action and cultivates positive relationships to maintain strong workforces when needed. As threats evolve, even educators and other leaders must keep learning and adapting to stay prepared.

Leading *through* a crisis is only needed, though, if the emergency happens. With continued research and analysis, some leaders look into the future to find ways to thwart crimes through environmental design, data management, technology systems etc. This December edition of the *Domestic Preparedness Journal* shares various ways readers (aka leaders) can build strength and resilience within their workforces and structures.

As another year ends and a new one begins, many people start thinking about New Year's resolutions. We can start with leading by example and asking ourselves: What would make me a better leader? How could I cultivate relationships and strengthen my workforce? What knowledge or skills can I share with others to better prepare them? What do I need to learn to build my skills and abilities? What programs, systems, structures, etc., do I need to update or change to prepare for and mitigate threats? Am I ready if I need to respond to a disaster?

The Importance of Strong Leadership for a Unique Discipline

By David Fogerson

Academics and consultants sometimes write leadership books without staff and constituent groups to demonstrate daily skill sets, emphasizing to readers where they are failing. However, biographies written by great leaders describing how they excelled, failed, and overcame failures provide pragmatic applications of leadership theories. For example, Theodore Roosevelt was a great leader who did some things wrong. Abraham Lincoln was a great leader who faltered in some areas but overcame them in others. Finding a balance between using leadership talents for good, improving skillsets, and making the world better is key to being a good leader.

Transactional vs. Transformational Leadership

Leadership theories typically fall into two main types: transactional and transformational. Transactional leadership is not well suited for leaders looking at the long game. Transformational leadership, which focuses on inspiring others to exceed requirements, is the better style for those in emergency preparedness and response roles. Planning for the long term requires making connections ahead of an incident and coordinating or combining resources across various silos for the public good. Meta-leadership is an example of pragmatically applying transformational leadership to the emergency management and homeland security enterprise.

At Harvard University's National Preparedness Leadership Initiative, Leonard Marcus, Barry Dorn, and Joseph Henderson use the cone-in-the-cube story when discussing meta-leadership to understand others' perspectives. Imagine a cube with a hole cut on the top and a hole cut on the side. Inside the cube is a pyramid. If one person looks through the hole in the top, they will see a circle. The second person looks through the hole in the side to see a triangle. They will fail if they do not communicate effectively and seek to understand why their views are different.

Emergency managers must lead across various silos to other leaders: the elected sheriff, county clerk, county manager, county commissioners, other fire protection districts, cities and towns, and nonprofit organizations, all of which are a necessary part of the enterprise but ones for which the emergency manager is asking for assistance, not directing. The following meta-leadership concepts apply to many situations:

- Look at yourself first;
- Lead up, down, and across silos;
- Lead outside your circle;
- Bridge with an emphasis to disband silos;
- Expand the role of entities; and
- Align disparate groups with a mission

Looking inward and using that energy from within helps to feed others and leads to successful leadership skills. The ability to both follow and lead is critical for meta-leadership to work. Consider the common firefighter mantra, "I am not here for me, I am here for us, and we are here for them." Being willing to be led when someone else has more influence, passion, and knowledge shows a leader's human side, builds trust, and demonstrates how each person's abilities are part of the bigger picture.

Emergency management is a unique discipline for leadership roles because emergency managers must look outward and lead in many unexpected situations.

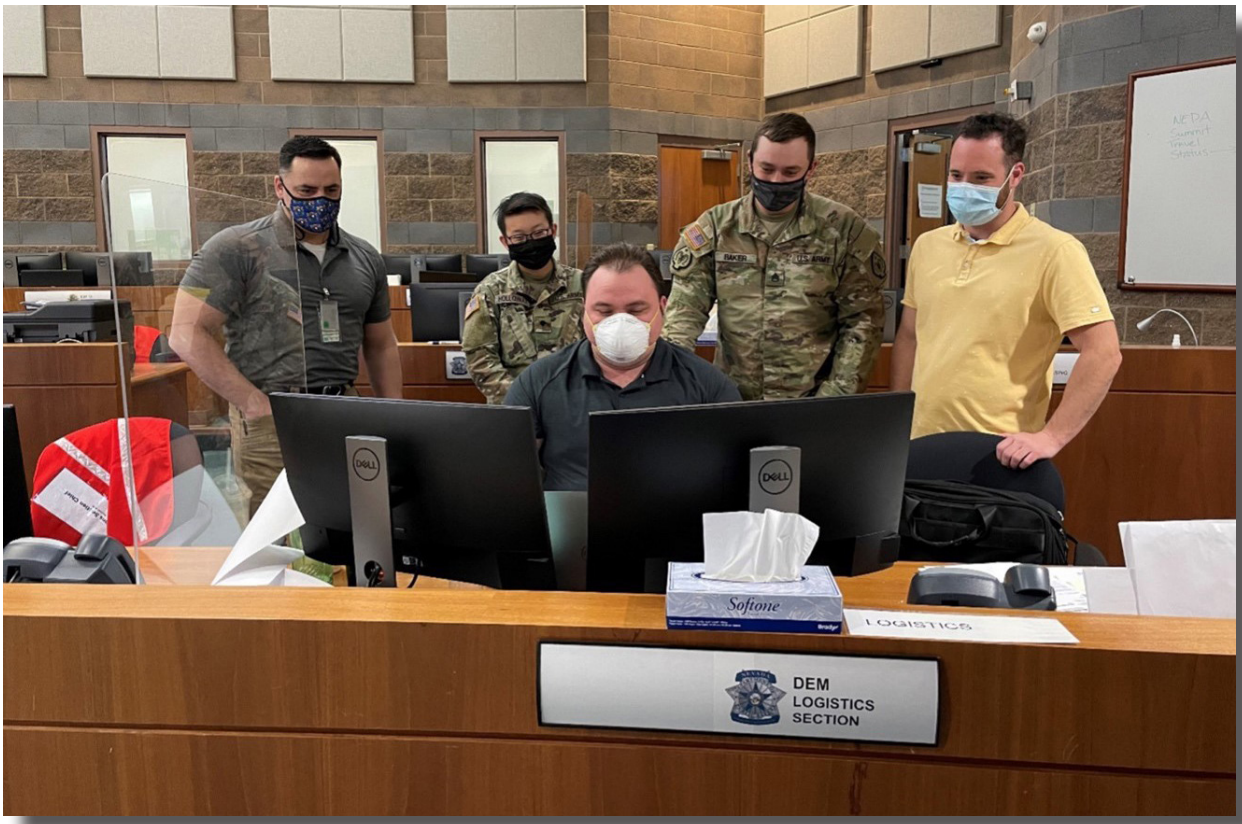
Many meta-leadership concepts focus on relationship building, which takes time. However, building trust and understanding others' visions, values, and goals allow the disparate groups to align during an incident. It is easier to be angry at "them" when there is a problem and more difficult to be upset with someone who is known and reachable by phone. This relationship-building can cause stress and derail collaborative cooperation if it does not occur before an incident.

Personal Lessons Learned as a New Deputy Fire Chief and Emergency Manager

At first, meta-leadership seemed depressing and irrelevant for a young deputy fire chief responsible for training and emergency medical services and emergency manager in a rural Nevada county. However, the importance of this concept soon became evident when considering the critical characteristics of these two roles. First, the paramilitary style of the fire service provides a deputy fire chief the ability to produce change, move resources, align funding with priorities, etc. Second, the emergency manager role has much responsibility but little authority across the silos. Telling other agencies what to do while planning special events caused some stumbles, so it was time for a new leadership style.

The COVID-19 pandemic tested the leadership skills of many agencies. In October 2020, testing was widely available, the vaccine rollout was close, there was much distrust of the government due to pandemic response efforts, there was an upcoming election, and that young deputy fire chief had just moved up to become Nevada's new state emergency manager. So the first task under new management was to rebuild trust within the Nevada Division of Emergency Management and with its partners. That took meta-leadership concepts:

- Showing vulnerability within the agency to allow others to step up and lead the organization;
- Implementing an aggressive travel schedule to reach each county emergency manager and health district to discuss the past, present, and future; and
- Establishing ongoing communication, owning issues, and resolving problems instead of just talking.



Bridging silos between Nevada, Nevada National Guard, FEMA Region IX, and the CDC Foundation at the Nevada Operations Center in 2021 *(Source:* Fogerson).

The simple act of a state official traveling to a local jurisdiction for a discussion during the pandemic had a positive impact and bridged silos across emergency management, public health, healthcare, local officials, and state officials. Those face-to-face meetings restored relationships that had broken down through the early days of the pandemic. Fortunately, or unfortunately, the pandemic lasted long enough for a reboot. Typical incidents do not provide the luxury of this corrective action time.

Meeting others on their home turf provides a better picture of the situation, a better understanding of others' organizational goals, and a feel for whether a stakeholder's words match their culture. For example, one rural county in Nevada appeared to be very much opposed to the vaccination efforts and required a visit. Once onsite, it became apparent that the oppositional voices were political while staff members were already hard at work conducting testing and vaccination clinics throughout the community.

Meta-Leadership's Role in the Unique World of Emergency Management

Emergency management is a unique discipline when it comes to leadership roles. While some agencies are inwardly focused, emergency managers must look outward and lead in many unexpected situations. Influence and credibility can grow when leaders

effectively manage incidents and lead up and across silos. However, as they assist others with leadership decision-making, they must be careful to avoid mission creep.

Internal to an organization, disbanding silos can improve communication and create a happier and more productive work environment. When everyone works toward one goal within an organization, an esprit de corps (feeling of pride and loyalty) is created. The same is not true for external agencies due to various hierarchical rank structures. The incident command system provides one way to communicate across operational networks, but the silos remain to some degree. For example, the sheriff's office is separate and distinct from the fire department as they have different missions, supervision, funding, etc. within each silo. However, a meta-leader can lead across the silos to ensure that everyone understands the roles and responsibilities each maintains.

Rather than breaking down silos, the barriers to effective communication, coordination, cooperation, and collaboration need to be removed. Through relationship building and being able to lead sometimes and follow other times, leaders create bridges across disparate organizations in various ways. Examples of a servant-leader could include:

- Bringing grant funding or resources to support local operations;
- Showing up at a long-term incident to offer food and rehabilitation supplies; or
- Being inquisitive about others' operations and seeking to understand how they operate to determine the best way to fit in and assist them.

Meta-leadership is a servant-leadership process. Emergency managers and other leaders should use meta-leadership concepts to establish relationships and expand opportunities to utilize connections proactively. For example, when an incident occurs or an event is planned, these relationships facilitate rapid team building to address the situation. Of course, it is overly optimistic to think that everyone on these teams will know each other, trust one another, and work to their full potential. However, the meta-leadership process will bring groups closer to that goal.

David Fogerson, MPA, CEM, is Nevada's emergency manager and homeland security chief. He leads the statewide agency to prevent, protect against, mitigate, respond to, and recover from disasters that are locally executed, state-guided, and federally supported. He is a Nevada Emergency Manager (through the Nevada Emergency Preparedness Association, NEPA), a Certified Emergency Manager (through the International Association of Emergency Managers, IAEM), and a chief fire officer designee. Prior to state service in 2020, he served as a deputy fire chief and deputy emergency manager for East Fork Fire Protection District in Douglas County, Nevada. He has 30 years of experience in the fire, emergency medical services, and emergency management arena. He received a Master of Public Administration from American Public University System and is a graduate of the National Preparedness Leadership Institute at Harvard and Centers for Homeland Defense and Security's Executive Leaders Program. Stewardship is important to him and to the future.

domestic preparedness

READERSHIP SURVEY

LEAVE US A REVIEW FOR THE NEW YEAR

CLICK HERE TO TAKE THE SURVEY

Maintaining a Strong Volunteer Force

By Kristina L. Hamilton

Volunteers are a lifeline for many nonprofit organizations and for-profit companies during emergencies and disasters. Volunteers tend to have big hearts for helping people and are willing to go out of their way to assist as needed. However, recruiting and retaining good volunteers can be difficult. Following are some simple strategies and tools for any emergency preparedness professional seeking to build and maintain a strong volunteer force.

Strategies & Tools for Volunteer Engagement

When recruiting volunteers, consider what the organization is looking for in a volunteer.

- Do they need to have a medical background with a current verified license?
- Is heavy lifting involved?
- Is there a lot of clerical work?
- What are the working conditions (indoor/outdoor)?
- What will they need to wear?
- What is going to be supplied?
- Are specific credentials or training required?

Once the event or task requirements are defined, the actual recruiting or assigning of volunteers begins. It is critical to avoid assigning a volunteer to a task or duty for which they are not qualified or overqualified.

One of the most important things to remember when recruiting volunteers is they are not getting paid to help. As such, with other personal and professional responsibilities, they may not be available to assist in every situation. COVID-19 was a good example. When the testing began, it was difficult to get volunteers as they were afraid to bring illnesses back to their loved ones. However, as more information emerged and the nation entered the vaccination stage, volunteers emerged from every direction.

As a result, the robust and trained team of volunteers that very smoothly ran the COVID-19 clinics came back to help at other clinics. Those volunteers performed essential tasks: helping with traffic, doing clerical work, giving vaccinations, entering data into computers, watching the people after their vaccinations to make sure they did not have any problems, taking clipboards off the nurses' stations, and cleaning and restocking the clipboards with new vaccination applications. They also cleaned the seats between visitors to maintain a sterile environment. For those who could not enter the

building, one of the clerical volunteers and a nurse would perform the tasks outside with the traffic volunteers observing those who received the vaccinations for 15 minutes and alerting staff if needed. Fortunately, no alerts were required outside or inside.

To retain volunteers, coordinators must respect this balance between commitments. For example, putting down a volunteer or implying they are untrustworthy because they cannot respond to every event would hinder volunteer retention efforts. However, simple, inexpensive strategies can work well in maintaining volunteers. For example:

- Praise them for their actions.
- Host an appreciation dinner or other event to make them feel wanted and needed.
- Express gratitude by saying "Good job" or "Thank you" to encourage them to return.
- Show personal recognition, such as sending birthday cards or thank you cards (some online websites can create cards and send them by email).

It is difficult for a threat preparedness volunteer coordinator or any other volunteer coordinator to recruit and retain good volunteers to fulfill roles that are not needed daily. There is only so much training that organizations can do to keep volunteers busy. During these downtimes are good opportunities for birthday cards and other friendly gestures to remind them that their services are appreciated even when they are not actively volunteering.

Volunteers tend to have big hearts and are willing to go out of their way to assist as needed, but coordinators must respect their balance between commitments.

The bottom line in retaining volunteers is to maintain regular contact. Ensure that the volunteers know they are needed and that they are doing a good job. In addition, the volunteers must understand the jobs they are doing for the events, disasters, or other efforts are being done well and that their efforts are essential to the success of the operations.

Getting Started

Various programs are available to help with grant funding for managing, recruiting, and retaining volunteers. There are even training programs for volunteer coordinators or managers of volunteers based on best practices. These training programs can be in person, virtual with online leadership, or online self-paced classes. Some state agencies offer grants and training programs to nonprofit organizations to help recruit and engage more volunteers. For example, in West Virginia, Volunteer West Virginia is the lead volunteer agency within the state's Department of Arts, Culture, and History.

Volunteers at a COVID-19 vaccination clinic at South Parkersburg Baptist Church, Parkersburg, WV (*Source:* Hamilton, March 10, 2021).

It is imperative to receive volunteer management training before starting a program that involves running a volunteer business or managing groups of volunteers. Another program that helps with volunteerism is the United Way of the Mid-Ohio Valley, which has staff that are friendly, available, and willing to help.

One more resource with information about many types of disasters, how to prepare for them, grants, help with volunteers, and so much more is Ready.gov. Much of their materials are free to order and can help facilitate organizing community emergency preparedness events. In addition, having volunteers helping at these events provides good opportunities for the volunteers to gain more familiarity with the topics in these materials.

Kristina L. Hamilton has been with the Mid-Ohio Valley Health Department since 2003 and currently serves as the threat preparedness volunteer coordinator. She also serves as the six-county regional volunteer coordinator for the Mid-Ohio Valley Medical Reserve Corps since 2011. In addition, she is a West Virginia Public Health Association member and a regional coordinator for the Community Emergency Response Team.

Implementing "Stop the Bleed" for Future K-12 Educators

By Will Brewer, Peggy Bergeron, and Wayne Bergeron



With just over 130,000 K-12 schools in the U.S. serving over 57 million students each day, schools are mostly safe places free from violence and danger where growth, knowledge, and learning happen, according to the National Center for Education Statistics. However, beginning in 2020, firearms-related incidents surpassed motor vehicle crashes as the leading cause of death for children in the U.S. School shootings are a uniquely U.S. problem that is increasingly concerning as both their frequency and lethality have increased over time. According to the Center for Homeland Defense and Security, there have been 2,052 school shootings since 1970, which have left 661 people dead. The worst year on record was 2021, with 249 incidents. The deadliest year in terms of casualties was 2018, with 51 people killed by violent intruders.

Since the Columbine High school shooting in 1999, school safety and security planning, as well as police and emergency response, have greatly improved. However, current statistics and media coverage show that school shootings continue to happen. Even the most prepared and well-resourced schools that have addressed recommended best practices in terms of safety and security may still face a school shooting incident and be forced to respond to and deal with the aftermath. Even with the most effective and professional law enforcement and first responder reaction, time can be a critical factor in who lives and dies during a school shooting. Faculty and staff preparation, training, and response can make a difference in survival.

Based on school shooting incident data, most casualties are caused by extensive injuries and uncontrolled bleeding from gunshot wounds. Death can occur within minutes of injury without appropriate response, including adequate treatment for bleeding. Most gunshot wounds cannot be treated with the simple first aid kits found in most school classrooms. Even if schools have the right equipment and supplies on hand, personnel must be trained and prepared to react to these types of wounds. Techniques to effectively control hemorrhages must be initiated accurately and with speed.

In 2015, the U.S. Department of Homeland Security initiated the "Stop the Bleed" program to educate the public on techniques to help control blood loss at the scene of the injury until the arrival of emergency personnel. The American College of Surgeons offers Stop the Bleed training, which includes trainers who provide trainees with a short slide presentation, discussion of bleeding control techniques, and return demonstration for the application of bleeding control techniques. After successfully completing the Stop the Bleed training, health

care and emergency management professionals are approved to teach the basic Stop the Bleed course. Approved Stop the Bleed instructors can collaborate with undergraduate K-12 education students to share knowledge, experience, and skills that can help save lives. This research study aimed to evaluate if the Stop the Bleed course was beneficial to future K-12 educators, as well as perceptions about career choice considering recent school shootings.

Method for Training Educators

Implementing steps to train non-healthcare individuals in life-saving skills can be challenging. However, after reviewing the curriculum for Stop the Bleed from the American College of Surgeons, the authors, two faculty members from the College of Nursing and one from Criminal Justice/Emergency Management at the University of North Alabama, decided training class should be implemented. After receiving instructor status with Stop the Bleed curriculum, these faculty members contacted the Dean of the College of Education to implement the Stop the Bleed training with the K-12 education students.

In August 2022, three class sessions were held for undergraduate K-12 education students to attend to learn life-saving skills that may be needed in their careers and elsewhere. The sessions were attended by a total of 66 K-12 education undergraduate students who were starting their internship in preparation for upcoming graduation later in the semester. The class followed the pre-designed format of Stop the Bleed with a PowerPoint presentation, demonstration, and return demonstration of skills. There are three main skills demonstrated in Stop the Bleed training: demonstration of pressure to a wound, packing of a wound, and application of tourniquets. The class was offered in a traditional lecture hall with a relaxed atmosphere where students were encouraged to ask questions, seek clarification, and be immersed in the training.

To appraise the effectiveness of the Stop the Bleed class with the K-12 education students, an exempt Institutional Review Board application was filed with the university and approved. None of the investigators have direct teaching responsibilities over these students as they are enrolled in a separate college within the university system. After the Stop the Bleed class session, the students were asked to complete a short anonymous survey consisting of four questions with additional demographic data items. The research team projected that the survey would take less than five minutes to complete. Informed consent was obtained on the survey before the questions were available

Participation by the K-12 education students was voluntary, and participation would not impact their status as a student at the university. A script approved by the Institutional Review Board was read to students at the end of the class. At the completion of the online survey, the students were provided a link to an outside site to register in a raffle for one $50 food/grocery gift card as a thank-you for participating in the survey. A random generator was used to choose the winner of the gift card. In addition, all students were issued an approved Stop the Bleed course completion certificate at the end of the class.

The following questions were presented to students using a QR code on a flyer that linked them to Qualtrics survey software:

- As a future educator, do you feel this course was beneficial to your career?
- Rate your confidence level in your ability to stop bleeding after taking this course.
- Please rate your fear of school-related shootings/mass casualties happening during your upcoming career. 0 means *no fear*, and 10 means *extreme fear*.
- Please share your thoughts, feelings, or beliefs about the recent school shootings related to your career choice.

The survey questions were generated to help the faculty understand if this training helped with confidence levels, and if the training was perceived to be beneficial. While the questions were brief, they provided the team with a good basis for future classes and gauging the confidence level of participants. Since the survey was online, the participants were able to answer the questions immediately after the class or at any location with internet access at their convenience.

In August 2022, three classes were held for undergraduate K-12 education students to learn life-saving skills that may be needed in their careers and elsewhere.

Because of the sensitive nature of the course content, several safeguards were in place. The students were warned at the beginning of the class that some images and topics may be graphic. The faculty also asked students to make the investigators aware immediately if they felt light-headed or faint during any part of the class. Finally, student counseling services were available if any emotional response to the training was experienced.

Results From Initial Cohort

Of the entire cohort, 89% (n=59) of attendees completed the surveys. The survey data was collected via Qualtrics software, which was used to aid the researchers in quantitative analysis. Data were extracted to Excel spreadsheets to view calculations of completed surveys, and descriptive statistics with one standard deviation were used to describe the data. The majority of the students that completed the survey were in the 22-25 years of age group (n=41). Most of the students that participated in the study identified as female (n=53; male: n=6). All students in the cohort had completed at least 90 hours of college coursework.

Overwhelmingly, 100% (n=59) of the surveyed participants felt this course was beneficial to their future careers as educators. Participants reported the following regarding confidence level in their ability to stop bleeding after taking this course: 44% (n=26) felt extremely confident, 49% (n=29) felt confident, and 7% (n=4) felt somewhat confident. Students expressed a high fear ($mean$=7.05, sd=2.31) of school-related shootings and mass casualties happening during their career when rating the fear from 1 (*no fear*) to 10 (*extreme fear*).

The participants also completed an open-ended question in the survey. The question asked the participants, as future educators, to share their thoughts, feelings, or beliefs about the recent school shootings related to career choice. The qualitative responses were analyzed with NVivo 12 software, which aided the researchers in organizing and coding qualitative data and resulted in four themes: "fear and anxiety," "importance of training," "preparation and readiness," and "no regrets about career choice."

Fear and anxiety – Overall, the participants expressed fear and anxiety related to their future teaching careers due to recent school shootings. Many participants indicated "scary to think that it could happen at my school" and "very scary to think about and I feel anxious about entering schools." One participant expressed a fear of death, "I am terrified that I may lose my life due to this." Another student stated concern with the level of support for educators, "I am scared and don't feel supported by the current education system." One student focused more on the safety of future students even while expressing fear of a possible school shooting, "It is scary because you just never know when and where it could happen. But, I know that I will do anything and everything to try to keep my students safe and out of harm's way."

Importance of training – Some participants indicated the need for more security for schools, as well as the importance of training for teachers. The future educators stated, "As a teacher, I think there should be more support and training given to all teachers," and felt "I believe more safety and protection could be provided to schools, staff, and students." Another participant shared, "The best thing for teachers is to have the proper training so that they can deal with the situation as best as possible." Several participants expressed gratitude for training such as the Stop the Bleed course, which was provided as part of this study. One participant stated, "I am absolutely heartbroken and devastated that a school shooting is such a reality in our country, but I am thankful for the various trainings available to be prepared in such an unthinkable situation." Another participant shared, "It is overwhelming to think about the possibility of experiencing this traumatic situation. However, after completing training I feel more prepared to act upon situations to the best of my abilities." Finally, one future educator noted, "It is extremely discouraging to think that one day I may be the only thing standing between the life and death of my students, but I am glad there are resources out there to teach us how to handle those situations."

Preparation and readiness – Preparation and readiness for possible school violence were indicated by the participants as, "We have to be ready at all times to protect our students," and "The only thing we can do is to prepare ourselves in case we find ourselves in a similar situation." One participant explained, "The recent school shootings have raised new anxieties and fears for my future students' safety. I want to protect them and for them to feel safe at school. In that situation I feel like I have some tools I can use to ensure safety." Another participant summed up the recent school shootings as follows, "It is insane that schools are being targeted for so much violence. It completely changes the culture of teaching and makes everyone reevaluate what it means to be a teacher…we are now facing the task of giving our students medical care for a gunshot wound or worse."

No regrets about career choice – The strong desire to still be a teacher negated any regrets about career choice for several of the participants. One participant shared, "As a teacher, it will be something I am prepared for, but I am not going to let fear control me." Other participants expressed, "I wish it didn't happen, but it does not make me regret choosing this career. I want to be the best teacher and keep my students safe," and "Our passion is to help students learn and make a difference."

A Need for More Classes and More Research

While this training was established in response to recent school shootings, it was stressed to the students as future K-12 educators that this knowledge was transferable to many situations that could require someone to Stop the Bleed. As a result of the implementation of Stop the Bleed class sessions with the K-12 education students, future sessions have already been scheduled for upcoming semesters. More research is needed on the preparation and training of future K-12 educators to handle the aftermath of school shootings. Emergency response organizations should consider reaching out to their respective K-12 schools to offer their expertise and training for programs such as Stop the Bleed.

Will Brewer, Ph.D., RN, CEN, CHSE, is an associate professor of graduate nursing at the Anderson College of Nursing and Health Professions at the University of North Alabama. Dr. Brewer is the director of simulation, which includes health professions and nursing (undergraduate and graduate). In addition to being a Stop the Bleed ® Instructor, Dr. Brewer is a certified emergency nurse, a certified healthcare simulation educator, and an advanced cardiovascular life support instructor. As a nurse of 20 years, Dr. Brewer worked in a large level 1 trauma center emergency room as a nurse prior to moving to academia.

Peggy Bergeron, Ph.D., RN, is an associate professor with the Anderson College of Nursing and Health Professions at the University of North Alabama. She has over 27 years of experience in the nursing profession in women's health/maternity, nursery, general surgery, post-anesthesia care unit, pediatrics, and college health. She currently teaches graduate courses in the Teaching-Learning Track.

Wayne P. Bergeron, D.Sc., Lieutenant Colonel, retired from the United States Army after a 23-year career within the Military Police Corps and Special Operations Forces. He currently serves as an associate professor teaching both criminal justice and security and emergency management and is the graduate coordinator for the Master of Science in Criminal Justice program at the University of North Alabama in Florence, Alabama. His education includes undergraduate degrees in criminal justice and political science, a master's degree in international relations, and a doctorate in emergency management.

Applying Environmental Design to Prevent Active Shooters

By Rodney Andreasen

Active shooter survival instruction has become a standard application within institutions to the point that it now rivals the training in the days of the Cold War for nuclear attack survival. "Duck and Cover" drills of the past have now become the "Run, Hide, and Fight" drills applied to classrooms, businesses, hospitals, and other entities. Law enforcement agencies and other first responders have developed response methods and tactics that have become routine and are effectively applied when these incidents occur. In the case of schools, the application of these tactics and methods increases as agencies practice response techniques, normally at the beginning of the school year. Active shooter training for teachers, workers, and others continues to accelerate to ensure people are ready to respond.

These trainings and response applications are essential and should be part of everyone's operational planning to survive attacks. However, one key piece has been missing for many years as the focus remains on response. Perhaps an event could be stopped or mitigated before it ever happens, thus reducing the need for the response or the application of these techniques. Again, the response and active shooter survival training are critical and should not be discounted. However, physical security measures or policies that were initially designed to stop the active shooter often fail.

The Robb Elementary shooting in Uvalde, Texas, warns of the dangers active shooters pose when preventative methods fail. Not every case will involve staff who have been properly trained in advance or have an immediate response from first responders. Therefore, the focus should be on a whole community application to prevent, prepare for, and respond to active assailants. Crime Prevention Through Environmental Design (CPTED) applications can provide one side of a triangle application process to stop or mitigate attacks. CPTED is not a new process but one that continues to find applications to numerous entities to help prevent incidents from occurring. CPTED can increase the security and ownership of an associated property or facility.

The International Crime Prevention Through Environmental Design Association defines CPTED as:

> *[A] multi-disciplinary approach of crime prevention that uses urban and architectural design and the management of built and natural environments. CPTED strategies aim to reduce victimization, deter offender decisions that precede criminal acts, and build a sense of community among inhabitants so they can gain territorial control of areas, reduce crime, and minimize fear of crime.*

4 Crime-Prevention Areas and Their Applications

Although this definition provides a basic application of CPTED theories to prevent crime, it goes much deeper and further in its application to prevent active assailants. CPTED applications comprise four primary crime-prevention areas:

- Natural surveillance,
- Natural access control,
- Territorial reinforcement, and
- Maintenance.

Natural surveillance is a way to observe, without obstruction, property under the control of or in use by the intended users. Although there are arguments for and against having numerous windows in a facility, more windows would allow for the observation of areas that may otherwise not be visible from the facility. Although excellent for many applications, closed-circuit television (CCTV) cameras may not supplant the surveillance capability of numerous people watching a specific area. Additionally, if individuals feel they are being observed, even though they may not be, they could be deterred.

Lighting is another aspect of this application. Although this may not impede an active assailant, it might deter criminal activity and illuminate areas others may use for nefarious reasons. Lighting is one of the most effective crime prevention applications in terms of cost savings and deterrence. Lighting systems utilizing light-emitting diodes (LED) are the most effective lighting systems available and provide cost savings through the longevity of the systems and reduced electricity costs. A lighting survey can be conducted for any facility to determine where lighting is lacking and what equipment is needed.

Natural access control reduces points of entry to a property through the use of various means – including vegetation or fencing – to obtain this objective. However, this does not mean turning a facility into a prison-like campus or high-security complex. Proper fencing can provide a deterrent to intrusion, territorial reinforcement, or additional reinforcement measures. In many cases, fences around facilities do not meet height requirements and provide little in the way of a deterrent. However, hostile vegetation such as Pyracantha (also known as Firethorn, Bouganvilla, or Rose bushes) can enhance the effect of fences and beautify the facility. Shrubbery, as previously mentioned, contains thorns and can deter, and preclude, individuals from even attempting to breach the fence.

Active shooter trainings can help prevent some injuries and deaths. Preventing the attack from occurring should be the ultimate goal.

Territorial reinforcement is a means of using items that show ownership by those occupying the identified space. As previously mentioned, fencing could form one aspect

of the process, along with landscaping, signs, and pavement treatments. Anything that can exhibit activity and creates an active space that shows ownership of the area and indicates delineation from public, semi-public, and private space will assist in this application. Even a small picket fence, or any of the previously mentioned hostile vegetation, can announce that the area behind it is private and provide the identified territorial reinforcement.

The final area involves *maintenance.* In its strictest definition, maintenance can be split into two specific applications as it applies to schools and school facilities. The first applies directly to maintaining the grounds where the school is located. Grounds that are unkept show that the facility is not valued and that the school may not care. Grass that is not cut or shrubbery not trimmed is a clear example of this belief. Additionally, landscaping that blocks the view of specific areas may lead to an incident occurring or prevent the identification of assailants trying to enter a facility. These issues can cause activity to continue until it is too late to respond, thus negating further prevention measures. Therefore, trimming trees and shrubbery to a recommended height to provide maximum observation are key considerations.

The second aspect of maintenance can involve the care afforded to the physical aspect of the campus. Graffiti left in place, doors and locking systems not repaired, or light systems not serviced, along with other aspects, invite issues that could have been solved by a simple fix or replacement. The cost of maintenance is far cheaper than the cost of paying damages required after an incident occurs.

Sadly, some argue that facilities cannot afford to implement such actions to prevent issues beyond the active assailant. There has been a great deal of overreliance on CCTV cameras and other devices to protect schools and other facilities. Although systems such as these are necessary, they can provide a false sense of security if not employed correctly and can create dangerous weaknesses in other areas.

Numerous studies have indicated that when schools and other facilities are turned into fortified facilities, the impact may override the learning environment as well as the working environment. There must be a healthy balance between learning and security, providing adequate protection for those attending school or working at a particular facility. The CPTED concept could provide a value-added aspect by reducing the feeling

of a prison environment while increasing the safety and security aspect for students, teachers, and other personnel. By using CPTED applications and including the students and teachers in the application, everyone becomes part of the ownership process for their school, facility, or organization.

CPTED applications, along with training for active shooter survival and proper response applications, should form a balanced program to prevent and respond to the threat of active assailants or other threats. A value-added aspect of CPTED applications can be achieved by increasing ownership by all who reside on the property and inside the facility, as well as providing a recipe for a successful protection program.

Facilities can no longer avoid applying principles and programs associated with CPTED. It is impossible to place a cost on the life of a student, a teacher, or an employee at any level; they are immeasurable. Considering the value-added aspect of CPTED applications for a school environment, the cost is minimal and should provide a pathway for increased protection, safety, and security.

Rodney Andreasen is a retired emergency management director from Jackson County, Florida. After serving approximately 20 years in that position, he retired in December 2020. Before that, he served 21 years in the Air Force, retiring as a Master Sergeant. He currently owns Xspct LLC providing consulting services on active shooter prevention and Crime Prevention Through Environmental Design. He is a graduate of the University of Southern Mississippi with a master's degree in Technical and Occupational Education, Auburn University of Montgomery with a master's degree in Justice and Public Safety, and the Naval Postgraduate School with a master's degree in Security Studies Homeland Security and Defense.

Value of Enterprise Data Management in Emergency Management

By Anne Marie Smith

An enterprise data management (EDM) program emphasizes the importance of managing information as an asset and protecting it from misuse or loss. Research by Gartner and similar services show that most enterprises and organizations carefully manage other assets (financial, physical, and human) but overlook the value inherent in their data. Typically, if an organization is cognizant of the data it captures, stores, and uses, it focuses on physically protecting the data through user access policies, controls on hardware and software, etc. – important aspects of data security. However, data security is not the only category of data management. Organizations frequently forget the need to understand what data exists in an organization, how to use the data, the purpose of the various data sources, and the roles that require data for operations and decision-making.

In an emergency management planning effort, or when an actual disaster strikes, knowing the landscape of data and how to manage it is critical to the organization's recovery and sustainability. For example, the lack of coordinated data about functioning shelters hindered residents' ability to receive essential services after Hurricane Sandy in 2012. Another example was the inability of organizational executives to access critical operational and analytical data to support re-starting business smoothly after September 11, 2001.

Developing a comprehensive program for managing data based on the commonly accepted functions of EDM would provide any organization, regardless of size or industry, with a central focus for identifying and controlling the collection, storage, management, and disposition of its data before, during, and after an emergency. Coordinating data management efforts with emergency management and disaster planning activities can enable organizations to recover more smoothly, allow critical operations to restart, and provide information for fact-based analysis and decisions.

Defining Enterprise Data Management

EDM is the global function that facilitates the management of data as an asset of an enterprise/organization. Dr. David P. Marco describes EDM's primary functions as follows:

- Data governance – planning, oversight, and control over the management of data and the use of data and data-related resources; development and implementation of policies and decision rights over the use of data
- *Data architecture* and *operations* – the overall structure of data and data-related resources to support data discovery, storage, and use;

- *Data security* – ensuring privacy, confidentiality, and appropriate access to data, and ensuring prohibition of inappropriate access or misuse of data and information;
- *Reference and master data* – managing shared data through standardized definition and use of common data across the organization;
- *Data warehousing and business intelligence* – enabling access to decision support data for reporting and analysis;
- *Metadata management* – collecting, categorizing, maintaining, managing, and delivering data definitions, calculations, descriptions, sources, etc., enabling "data knowledge"
- *Data quality* – defining, monitoring, maintaining data integrity, and improving accuracy, completeness, validity, timeliness, and consistency of data.

Recognizing that most organizations did not plan their information technology (IT) environments holistically, redundancy and omissions in data, process, and technology exist throughout almost every company. Many organizations do not include data management in their disaster recovery or emergency planning efforts or only focus on restoring tangible hardware, network, and software assets, omitting data accessibility as a critical aspect of recovery.

The role of EDM and the management of information from an enterprise perspective are essential to any successful organization. EDM optimizes the corporate information assets for the business user and the IT community.

EDM practices can play a vital role in any disaster recovery evaluation or emergency management effort. Essential parts of EDM, such as metadata management, data governance

and stewardship, and master data management, can support more comprehensive emergency planning. A robust EDM practice can enable organizations to recover more quickly from a disaster since their data is managed with continuity, organizational consistency, and protection as focal points.

The involvement of disaster recovery and emergency management specialists is essential in assessing the value of the information resources since many organizations' most vital asset after their people is their data. Data management professionals can provide training in the basics of EDM and its foundational components (data governance, metadata management) for disaster recovery and emergency management professionals. Understanding the purpose and value of EDM can help disaster recovery and emergency management staff work with data management professionals to assess the requirements for using data to support recovery efforts. As an essential function in EDM, data governance programs can become a fulcrum around which disaster recovery and emergency management planning and recovery initiatives programs revolve, providing the organization with secure, accurate, and timely access to data to help restore operational capabilities.

The involvement of disaster recovery and emergency management specialists is essential in assessing the value of the information resources before a disaster.

Data and information security is another essential component of an EDM program. The need to involve emergency management and disaster recovery planning in designing and implementing data security policies and processes is paramount. In the final analysis, developing an EDM program that includes emergency management and disaster recovery efforts would organize and protect the organization's data – an often overlooked but vital asset. Some action items for emergency management professionals could includes:

- Discover what data management programs/efforts exist at the organization, become familiar with its approach to data management, and how these functions can support emergency management and disaster planning.
- Educate data management professionals in the organization about the essential aspects of emergency management and discover alignments with data management functions such as data governance policies, data architecture, and operations, data security, etc.
- Collaborate with data management professionals about how to include planning and recovery activities for computer hardware, networks, and software, and develop plans for effective data recovery and access for all emergency planning and disaster recovery scenarios.

Anne Marie Smith, Ph.D., is a leading enterprise data management consultant and a frequent contributor to various publications on data strategy, data governance, data literacy, and data security. She has over 20 years of experience in data management for several organizations and has successfully led the development of data management departments within corporations and consulting organizations. She earned a Ph.D. in Management Information Systems (MIS) from Northcentral University and has served as a university instructor and course developer. In addition, she holds several certifications in data management and related areas.

How Technology Systems Impact Critical Infrastructure

By Nathan DiPillo & Paul Galyen

Disaster movies of the 1980s and 1990s attempted to predict the "end of times" due to a major computer systems failure, including fears over "Y2K." One of the reasons the premise of these movies seemed plausible is that understanding the nuances and impacts of compromised operational technology (OT) systems on critical infrastructure is more of an art than a science. From social media and online work environments to microchips under the skin to validate user identities, society is increasingly dependent on information technology (IT) to sustain life. As IT dependency affords many security challenges, OT supporting critical infrastructure is no less important and, in many ways, more so. For example, people can survive without social media for a month, but not water. However, OT is taking longer to catch up to IT and modern security challenges. OT systems are designed to run and operate for much longer cycles than IT systems, 30+ years or more, depending on industry growth. This is key when understanding the differences and the reliance critical infrastructure has on OT systems.

The National Institute of Standards and Technology states that OT "encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events." This process was simple in the 1860s, with punch cards controlling textile machines. However, since the 1950s, technology and the ability to build "widgets" faster and smaller has led to significant advancements for all the right reasons in the OT world.

Regulatory oversite for OT in the energy sector is guided by FERC/NERC, whose efforts focus on network monitoring sensors, centralized collectors, and information-sharing practices. Although these efforts are encouraging, other sectors do not have the same regulatory oversite or cyber enforcement, hindering resilience between the cyber-physical ecosystems. The impact of the COVID-19 pandemic made this situation worse. Due to teleworking mandates and remote work environments, these measures forced some owner-operators to use remote access tools to manage OT. This quick-fix response using *industrial internet of things* or IT remote access systems opened the door to more attack vectors and compromised OT systems.

The Target data breach of 2013 highlighted the risks of having OT and IT systems on the same network. The breach was successful because a third-party heating, ventilation, and air conditioning (HVAC) vendor used a remote access solution that was not secure.

As a result, the HVAC network provided a path for the attacker to gain a foothold into Target's point-of-sale network, which resulted in the theft of data on over 110 million Target customers.

Over the past 50 years, IT's developments and fast-paced innovations in flexibility, availability, and security have lapped the OT environment. OT may be unable to catch up without radical changes, regulatory oversite, and significant sacrifices by companies and agencies. According to Tripwire, IT/OT security can be challenging:

> *[I]t's not realistic to apply cybersecurity best practices from the [IT] side of your organization to the [OT] side. IT and OT environments consist of completely different types of devices and network structures. OT environments also experience wildly different risks and threats than IT environments.*

The risks and costs to mitigate these threats are driving different equities of how companies and agencies invest in protecting these ecosystems.

Connecting OT to critical infrastructure systems is defined using Industrial Control Systems (ICS), which are the onsite or remote systems that control hydroelectric dams, energy infrastructure, chemical plant operations, transportation systems, food and agricultural operations, communications, and other critical infrastructure assets. There are three classes of ICS: Distributed Control Systems, Programmable Logic Controllers, and Supervisory Control and Data Acquisition (SCADA) systems. These three classes define how OT interacts and functions with the physical side of infrastructure – for example, moving valves, operating sensors, controlling/measuring flow, etc. Some processes use digital and analog signals depending on how the software interacts with physical hardware or how the switch moves a valve. These two communication mediums present security risks and are a major gap where many vulnerabilities hide.

Source: iStock/ ipopba

According to a Forescout report in 2022, OT "vulnerabilities are divided into four main categories: insecure engineering protocols, weak cryptography…, insecure firmware updates and remote code execution via native functionality." In the same report, Forescout's Vedere Labs discovered 56 vulnerabilities from ten OT equipment vendors that provide systems to critical industries, such as oil and gas, chemical, nuclear, manufacturing, water treatment and distribution, and mining. Many vendors sold these systems as "secure by design" or "certified" with OT security standards. However, the security evaluation of these systems proved otherwise.

Lessons Learned

Two recent cyber incidents provide valuable lessons. In February 2021, a threat actor gained access to a Florida city water treatment plant's SCADA control system and manipulated the amount of sodium hydroxide introduced into the system. Fortunately, plant personnel noticed the change and corrected the issue before the water became toxic. The reported vulnerabilities were an outdated Windows operating system and poor password management that leveraged TeamViewer software and allowed remote desktop access. In another 2021 case, Colonial Pipeline decided to proactively shut down its ICS system in response to a ransomware attack on its IT system. Unfortunately, that shutdown caused cascading disruptions and delays in the pipeline's logistical supply chain.

One of the most notable incidents in recent history is the attack on Ukraine's energy infrastructure. In 2015, Ukrainian power companies experienced unscheduled power outages impacting many of their customers. Threat actors used a combination of OT and IT vulnerabilities to compromise the Ukraine power grid. The threat actors used a "spear-phishing" attack against the Ukraine utility company, which installed malware to seize the utility company's SCADA control systems, subsequently shutting down the power substations. Next, the attackers targeted the utility company's IT infrastructure components – including uninterrupted power supplies, modems, and remote terminal units – and the emergency power supply at its main operations center. Reports stated the attack shut off 30 power substations, impacted over 230,000 customers, and turned off power in some areas for one to six hours.

Understanding Fundamentals

Understanding the fundamentals between IT and OT systems is a good place to start in assisting agencies and companies with being better prepared to mitigate and respond to threats and attacks on critical systems. Instances of retired persons returning to work to teach new and current employees how to bypass a compromised or inoperable OT system – for example, manually turning on or off valves or switches using hand tools – are becoming more common. With the *great resignation* still looming, it is time for employers, companies, and even governmental agencies to discover, collate, document, and train on this legacy knowledge. Failing to do so now may permanently lose the tacit knowledge needed in an emergency.

These stories are abundant in the kinetic world of infrastructure, especially in long-standing systems like water, energy, and transportation. Since OT is older and designed in an era when technology was not as advanced, there have been fewer updates. Although some OT systems are not connected to the internet, organic vulnerabilities remain because threats have changed. Understanding how the networks are connected and how the workflow is handled is one solution to discovering vulnerabilities and c-suite staff understanding how to protect company property, IP (intellectual property), and brand reputation. According to Tripwire, there are three risk factors to consider:

- *Unintegrated technologies* – Many ICSs are purpose-built, proprietary, and created when cybersecurity impacts were not a concern.
- *Flat networks* – Many ICS networks are flat, meaning each device has access to the rest of the network. In a flat, non-segmented network architecture, a malware attack against one device allows the malware to propagate through the control environment with impunity.
- *Workforce challenges* – A skills gap for securing ICS has emerged through an aging workforce and the adoption of IT technologies within ICS at a faster rate. With an estimated 3.5 million unfilled cybersecurity jobs by 2014, the skills gap is another challenge to overcome.

Cascading impacts of *industrial internet of things* or IoT (internet of things) systems coming online quicker than staff can be hired, oversimplification of systems' security protections with one IT person having administrative access to all systems, technology moving faster than industry standards can keep up, plus a looming skill, knowledge, and ability gap growing with an aging workforce, and fewer people going into the trades create a perfect storm for catastrophes. In addition, with more successful cyberattacks and possible long-term economic concerns pushing this narrative, the industry is not fully prepared. For example, many independent service operators in the energy industry can re-route electrical supplies and effectively monitor the system, but there are still significant gaps. ASCE's 2021 Infrastructure Report Card states, "The electric grid is becoming more vulnerable to cyberattacks via industrial control systems, consumer Internet of Things devices connected to the grid's distribution network, and the global positioning system." With natural and person-caused threats and hazards to infrastructure, specifically, lifeline critical infrastructure, being prepared now will mitigate the loss of life and economic impacts.

With IT's developments and fast-paced innovations, OT may be unable to catch up without radical changes, regulatory oversite, and significant sacrifices.

Solutions and Action Items

Although separating IT/OT systems also has been adopted as a threat mitigation strategy, some companies are now combining them again to help with overall cybersecurity. According to the Center for Internet Security, there are some simple solutions to consider:

- Ensure firewalls are configured to deny by default.
- If a location is not staffed or critical process data flows through a perimeter device, ensure that redundancy exists and that device failure will not prevent this data from being received by its intended destination.
- Ensure systems are kept up-to-date and pay attention to security patch releases, vulnerability notifications, and firmware releases. Unsecure services, poor firewall configurations, and default credentials remain issues.
- Use the principle of *least privilege* – only grant access to data and systems to those that require it.
- When leveraging an IT-based security information and event management solution, ensure that it supports the ICS environment because many logging analytic and alerting solutions do not support or correctly interpret or correlate ICS-specific events.

Lastly, staying informed about emerging threats, vulnerabilities, and cybersecurity tools and resources is critical to mitigate threats and shorten the return time to a "cyber normal." Categorizing systems into simple processes and discussing solutions around this process might help owners and operators tackle the prioritization challenge:

- Older un-interrogatable ICS/SCADA systems (know systems that need to be updated and or cannot due to operational software boundaries);
- Current/existing ICS/SCADA system (these can be a combination of older and newer systems, those that have had past updates or have the potential of adapting new ICS/SCADA systems); and
- Future or advanced integration of ICS (these are systems being updated or proposed to be updated by choice or regulation).

Preparedness professionals have options for sharing knowledge and facilitating changes to mitigate IT/OT threats. For instance, organizational leaders can become members of the Information Sharing and Analysis Center (ISAC). In addition, procurement officials can leverage contracts to incorporate IT/OT threat mitigation. For example, firmware updates for new security cameras can be included within a new contract vehicle in order to avoid additional costs or delays when future updates are needed.

The future of IT/OT systems is improving, with more resources and monies dedicated to this space. Under the guidance of the Cybersecurity and Infrastructure Security Agency (CISA), the federal government warns owners and operators of "critical infrastructure OT

and control systems assets to be aware of current threats we observe, prioritize assessing their cybersecurity defenses and take appropriate action to secure their systems." The House passed the DHS Industrial Control Systems Capabilities Enhancement Act of 2021 (Bill H.R. 1833), which guides CISA's National Cybersecurity and Communications Integration Center to ensure that its activities address the security of both IT and OT, including ICS. These efforts in Congress continue under the direction of the Department of Homeland Security.

In California, cybersecurity is a top priority. The California Cybersecurity Integration Center is part of a growing effort to centralize and mitigate cyberattacks, offer solutions, and provide education to the public and other state agencies. Across the nation, federal and private entities are engaging in the cyber-to-physical space, with more small and large agencies and companies taking notice. Small rural critical infrastructure owners and operators are getting solutions with options for cybersecurity grant programs.

Looking at threats from an all-hazards perspective is the future of how emergency managers, cyber response agencies, and private entities can tackle the convergence of cyber-physical threats. *Cyber-physical systems* is a new buzz phrase to help group the problem and support resilient OT systems. With the ever-decreasing gap between the cyber and physical worlds, efforts across industries and governments must be streamlined to prepare for, mitigate, and respond to these threats. Continuing the conversation and allowing for data sharing and trust is paramount to ensuring that the lights stay on, the water keeps flowing, and life continues thriving.

Nathan DiPillo currently serves as a California Governor's Office appointee assigned to the California Office of Emergency Services as a Critical Infrastructure Analyst in the State Threat Assessment Center. Before state service, he functioned as a critical infrastructure specialist with the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA). He also spent over 15 years with the Transportation Security Administration, where he assisted in standing up the agency with policy development, training, and recruitment. He has over 25 years in the emergency management and security industry, beginning as a resident firefighter/emergency medical technician. He also served with the California State Military Department, Army National Guard in the 223rd Training Command ending his career as a Sergeant First Class. During that time, he served in many units, finishing his career attached to the 102nd Military Police Training Division in an Opposition Force Unit. He served as a career coach with HireHero's USA and assisted in coordinating an emergency family communications group in his local area. He possesses a Master of Emergency Management/Homeland Security from the National University and other Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security (DHS), and military certifications. He currently serves as an advisor to the Domestic Preparedness Journal.

Paul Galyen, CISM, is an experienced information security professional skilled in vulnerability management, security architecture, and endpoint security hardening, currently working with the California Cybersecurity Integration Center. Before state service, he worked as a contractor providing cybersecurity and digital forensic analysis for a large IT company and a major aerospace company. In addition, he served eight years as a communications specialist with the United States Army Reserve with the 801st Engineering Company (Horizontal Construction) and the 305th Engineering Company (Route Clearance), including a military deployment to Afghanistan in 2014 in support of Operation Enduring Freedom. He received a Master's of Information Technology Management with a specialization in cybersecurity from Colorado State University Global Campus.

ARTICLES OUT LOUD FOR YOUR BUSY LIFE

Emergency Preparedness Professionals are incredibly busy and often on the road. To give you more opportunities to benefit from the articles in the Journal, you now have access to Articles Out Loud that will be available for a trial period.

You can find our first Article Out Loud on our website under the Podcast channel, or in the iTunes store.

Don't forget about last month's Journal! Click **HERE** to download it now.

DON'T MISS ANOTHER ISSUE OF THE DPJ WEEKLY BRIEF OR THE DOMESTIC PREPAREDNESS JOURNAL

Subscribe Here