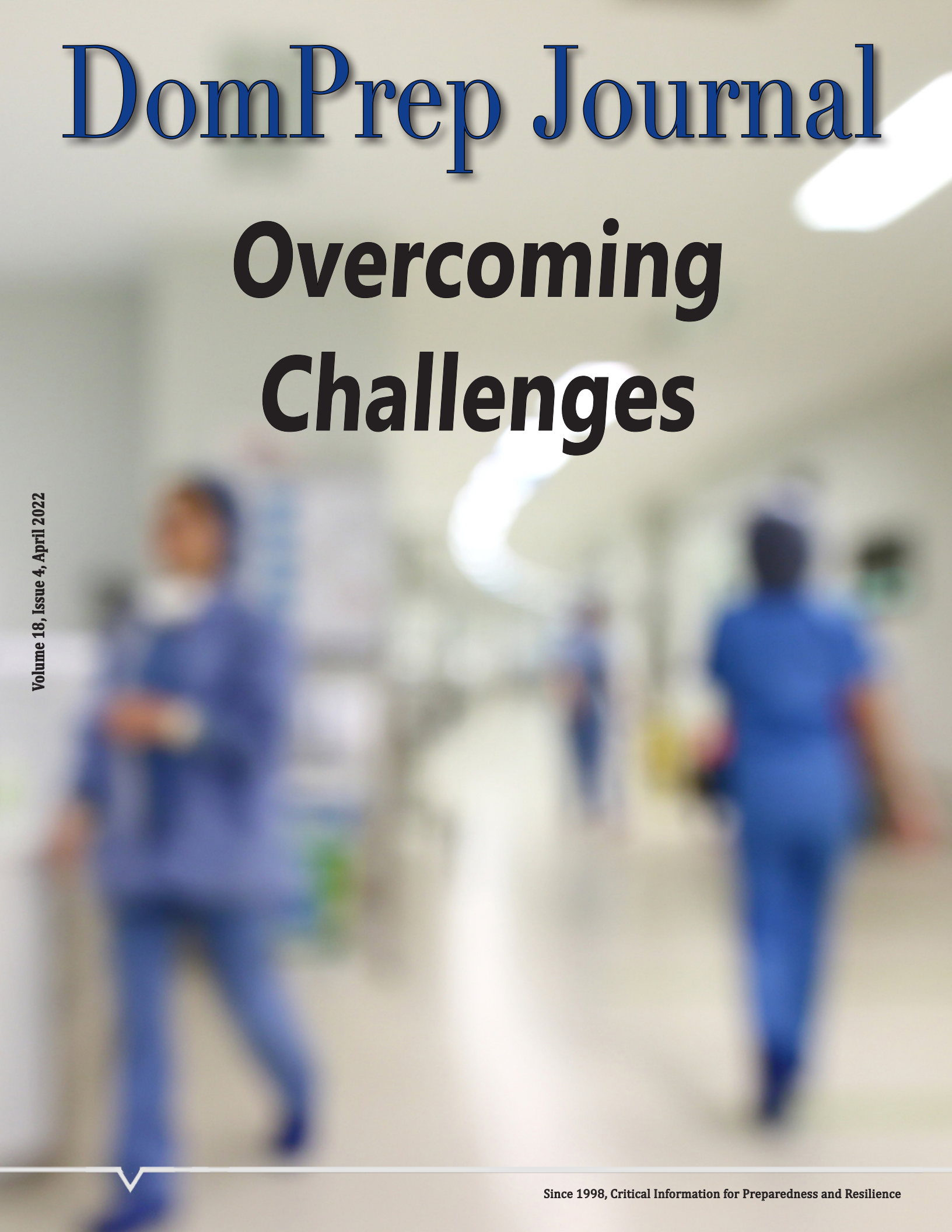
DomPrep Journal

Overcoming Challenges



Volume 18, Issue 4, April 2022

Since 1998, Critical Information for Preparedness and Resilience



Partner with the world-wide leader in emergency preparedness and response solutions

Juvare connects more than 95% of the U.S. population through its emergency preparedness and response technologies, including **WebEOC.** As the world's most widely-used, battle-tested emergency management software, WebEOC empowers users to prepare for and respond to emergencies with features built for any user, at any skill level.

- **Unrivaled flexibility** with built-in tools and an open API that enable you to customize the solution to your organization
- **Enables efficient collaboration** though data-sharing and common workflows across agencies, geographic boundaries, and both public and private sectors
- **Faster alerting** though WebEOC Alerts Plugin, with notifications that meet responders where they are most easily reached
- **Emergency preparedness expertise,** with a deep understanding of the needs of our partners across federal, state and local agencies, healthcare, corporate, non-profit and education

Visit *juvare.com* to learn more about WebEOC and other flexible solutions to meet your unique emergency preparedness and response needs.

JUVARE



Business Office
1033 La Posada Drive
Suite 135
Austin, Texas 78752
www.DomesticPreparedness.com

Staff
Texas Division of Emergency Management
Publisher

Catherine Feinman
Editor
cfeinman@domprep.com

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

Advertisers in This Issue:

Juvare

International Association of Fire Chiefs (IAFC) Hazmat Conference

Domestic Preparedness Journal is electronically delivered by the Texas Division of Emergency Management, 1033 La Posada Drive, Suite 135, Austin, TX 78752, USA; email: subscriber@domprep.com.

Featured in This Issue

Pictured on the Cover: Source: ©iStock.com/ OZANKUTSAL

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

SUSCRIBE **HERE**

Overcoming Challenges – Do Not Skip Steps

By Catherine L. Feinman

The nation faces numerous natural, human-caused, and technological threats. As threat environments change, efforts to prepare for and respond to them must also evolve. To overcome many of the preparedness challenges that communities currently face or will face in the future, leaders should take a two-step approach: Step 1, identify the threats, hazards, and risks; Step 2, take actions to mitigate these threats, hazards, and risks. Of course, this simplified approach is not at all simple, but it is necessary for reducing the impact when an emergency or disaster occurs.

Imagine skipping one or both steps – for example, a community in a flood zone without an evacuation plan, or a hospital's robust security plan to keep out intruders when an insider attack occurs. Whether because of budget allocations, limited resources, lack of interest, politics, or some other reason, some communities and organizations are still skipping steps. However, these daunting tasks are not single actions but rather a never-ending process of evaluation and improvement.

Identifying threats, hazards, and risks is an ongoing process that requires leaders to be on alert for anything that may affect their current emergency plans and procedures. As COVID emerged, healthcare providers faced many new challenges such as resource deficits and workforce retention that left many facilities unprepared. They also are facing the growing threat of active shooters and other violent incidents. Critical infrastructure is another sector that is vulnerable to both cyber and physical attacks. By identifying the threats, leaders can begin to take actions to secure and protect their facilities and communities.

Taking actions to mitigate the threats, hazards, and risks is also an ongoing process that requires leadership support, stakeholder buy-in, and resources. Redundant communications systems are one way that communities can ensure interoperability when one or more modes of communications are affected. Training and education can help promote stakeholder buy-in and build the human resources needed to respond to current and future incidents. Internships are just one of the training and educational opportunities that can sometimes be overlooked for recruitment and professional development.

In this April edition of the *Domestic Preparedness Journal*, the authors provide valuable information to get leaders focused on overcoming preparedness challenges. Through identification and action, communities will be more resilient to future emergencies and disasters.

Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as editor of the Domestic Preparedness Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and recovery communities. She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

A Growing Threat to Healthcare and Other Facilities

By Rodney Andreasen

Shooting incidents and other attacks seem to be increasing. In many cases, domestic violence has become a common denominator and one that has many opportunities for prevention. While the domestic violence threat alone is tragic, these incidents can become more deadly when they transcend the home and enter the workplace, resulting in secondary victims being harmed. Perpetrators who are unable to vent their frustrations on the intended target may transfer their aggression toward others who simply get in the way.

Active Shooter & Violent Incidents

Numerous facilities such as nursing homes, assisted living facilities, and small outpatient clinics have become targets of violence. Here are just two of the numerous examples that span the country.

On May 12, 2017, the small community of Kirkersville, Ohio (population ~500 at the time) was rocked by a violent encounter. Much like other small communities around the nation, Kirkersville never expected a criminal act of this nature. A routine day ended with an event gone tragically wrong as a nurse who worked at the local nursing facility became a domestic violence target. Several other individuals present simply got in his way. The new police chief, who had been on the job for three weeks, responded and was killed in an ambush by the assailant. The assailant then forced his way into the facility where he confronted and killed a nurse's aide. The assailant then moved through the facility in search of his ex-girlfriend. The assailant found and killed her, then took his own life. A search of his home after the incident revealed more than 60 firearms he had purchased or come into possession of despite his extensive criminal history and record.

While protection from domestic violence is paramount, another threat has emerged. Much like domestic violence, the insider threat provides another unique challenge for planners. On February 4, 2021, the city of Lafayette, Colorado (population ~34,200 at the time) saw such an incident take place at a nursing home facility. Reports indicate that a resident of the facility had shot and killed the maintenance man, whom the shooter accused of stealing his money. His attack was methodical in nature as the resident watched his victim complete his safety checks and then shot and killed him. The killer was a 95-year-old resident of the facility who made numerous threats in the past as well as statements to the effect that he was going to kill people. Most interestingly, he had a firearm in a facility that did not allow them, and the facility staff had previously disarmed him on another occasion.

Small facilities like these have increasingly become targets of malicious acts of violence. However, violence is not limited to assisted living facilities or nursing homes. Other medical entities are also targets of various types of violence, including small outpatient clinics.

An Expanding Threat With Significant Consequences

With medical facilities continually having to deal with increased patient loads and shortages of medical personnel, the chance for violence against doctors, nurses, and other support personnel can and has increased exponentially, with healthcare workers accounting for about half of workplace violence victims, Statistics that are tracked each year show that the type of violence most prevalent in these facilities is Type 2 Workplace Violence. The National Institute for Occupational Safety and Health (NIOSH) identifies this as violence from a customer or client, including patients, their family members, and visitors directed toward healthcare personnel.

With the emergence of COVID-19, which led to many being confined to their homes, there has been an increase in violence across the spectrum. As dangerous as this occurrence is, there is a potential for this type of violence to occur in other medical venues separated from the primary facility. This threat involves those that may serve smaller communities or provide outlier medical services on a 24/7 basis.

For example, on February 9, 2021, five people were shot (one later died) inside the Allina Health Clinic in Buffalo, Minnesota (population ~16,700 at the time). The clinic was a small outside facility that provided outpatient care. With numerous events of active shooters occurring across the country in numerous venues, increasing threats against outpatient and other associated facilities can be overlooked. Much like the increase in attacks against houses of worship, places of healing should become more aware of such direct and indirect threats, regardless the size of the community.

Outpatient clinics and those that may provide services in a 24/7 emergency capacity could become a new category of facility to experience violence. In many cases, these facilities are minimally staffed and may not have security staff present to deter crime and secure the facility. Some facilities have never had a security assessment or other review of the structure, which may deter or prevent crime. Some buildings may have been used previously for other functions or may be located in relatively high-crime areas. Consequently, these facilities provide a dangerous combination of conditions where an attack of a personal or non-personal nature may take place.

The threat is real, and the consequences can be high with a major loss of life. Regardless the size of the city or facility, shootings and other attacks can happen.

Guidance for Preparedness & Repsonse

There is no one-size-fits-all application and no perfect program that can prevent every action from taking place. However, some processes and programs can be applied to mitigate the threat. For example, information garnered from previous incidents can be used as a guide for preventing them from occurring in other organizations. Although no two organizations are the same in form or function, there are enough similarities to benefit from examining others' failures and applying lessons learned. The Department of Homeland Security developed such a program many years ago to look at individual

incidents and programs to provide a lessons learned database for organizations to research. The same should be developed for medical organizations or those providing assisted living services. The Lessons Learned Information Sharing (LLIS) can still be accessed through the Naval Postgraduate School CHDS program.

Next, the employment of Crime Prevention Through Environmental Design (CPTED) could be added as a method to assist in designing the environment that would make the facility and surrounding area less of a target for a criminal element. This could also make it more inviting for the local population to use. CPTED, although an older concept, is one of the best methods available to "design out" crime. The process has become so engrained in applications for safety and security that it has taken on new applications in the prevention of terrorist attacks. The programs associated with this concept work and have had a positive impact across the spectrum.

In concert with CPTED should be the application of a risk assessment to address current physical security aspects of the facility as well as the current procedures and policies that are applied thereof to perform emergency and day-to-day functions. The CPTED concept and risk assessments complement each other in their application. The risk assessment examines external and internal issues that may promote or prevent violence in the facility. Assessments of this nature should be completed by a certified CPTED and/or risk assessment specialist. A list of CPTED certified specialists can be found at the National Institute of Crime Prevention (NICP).

Training is another aspect that should be developed to prepare personnel in the facility. For many years, training on active assailants has been conducted under the guise of the active shooter. However, many points are still missed that apply to an active shooter event. These need to be addressed. Active shooter training is important and should be continued, but areas contained in an Active Shooter Hostile Event (ASHE) program should be expanded beyond just that scenario.

Areas that should be covered and made available to everyone in the immediate area include Stop the Bleed®, CPR and AED programs, and the development of Stop the Bleed kits. The National Fire Prevention Association (NFPA) provides guidance to assist in the development of programs within medical and assisted living organizations. Making situational awareness instruction a requirement for all personnel would not only assist individuals while operating in the medical facility, but it also would apply to their daily lives outside the facility. This type of training is a value-added process that builds awareness of potential dangers inside the facility, outside in the parking lot, or in public areas like malls.

Finally, facilities should establish a See Something, Say Something program, which makes everyone responsible for the safety and security of personnel inside and outside the facility. The program has been successful at many levels and can be applied in daily operations.

These suggestions do not cover the entire set of programs that may be needed at any specific facility because each facility is unique. However, the danger is real, and more effort is needed to ensure that threats inside and outside an organization are identified and planned for when possible. The development of a threat matrix and a multiyear training plan can help organizations meet their training needs. Each effort an organization makes is one more step in preparing individuals to be safe. As a guide, organizations should look to the International Association for Healthcare Safety and Security (IAHSS) for suggestions.

Real Threats With Significant Changes

The threat of active shooters and other violent incidents is real, and the consequences can be high with a major loss of life. It does not matter how large or small a city is, how large or small a facility is, or what the major function of a facility is at present. Shootings and other attacks can happen.

While each type of incident mentioned above can be viewed as isolated in nature, these examples indicate the myriad of threats that hospitals, medical centers, smaller outpatient clinics, nursing homes, and assisted living facilities can face. Organizations must look at threats beyond that of active shooters. When entities focus on one specific area, the threats that exist from other entities become blurred. It may become clear when an incident occurs, but by then it is too late. Planning must be a whole community process and include everyone concerned. By doing this, everyone becomes part of the planning and will be able to better identify and prevent incidents from happening.

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 as well consulting with the Counter Threat Group LLC in Birmingham, Alabama. 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.

Securing & Protecting the Nation's Cybersecurity Infrastructure

By Chandler Lofland & Raymond Walker

The Colonial Pipeline cyberattack in May 2021 exposed the urgent need to safeguard and upgrade the critical infrastructure systems in the United States. Congress acknowledged that the government lacks the authority to require private companies – which own, operate, and protect 85% of the nation's critical energy infrastructure assets – to adopt the necessary levels of cybersecurity. The cyberattack underscored how vulnerable vital infrastructure industries are to assaults on virtual computer networks, exposing a failure to avert attacks on private energy sector partners.

The economics of providing cybersecurity have become a significant challenge due to finite resources that could limit or reduce attacks targeting U.S. industries on private infrastructure networks. Additional comprehensive congressional legislation to enforce greater private industry reporting parameters is needed but has often failed due to partisan disagreement and the inadequate resources of private sector entities.

Laws, Policies, and Historical Background

There is debate within cybersecurity circles that the Department of Homeland Security (DHS) could be far more effective in providing security alongside its missions of traditional protection roles. DHS should focus more efforts on coordinating cybersecurity and critical infrastructure requirements to bridge the growing gap between publicly and privately owned and operated infrastructure systems and attempt to have federal cyberprotection efforts extend to all energy sectors. This new focus could rebalance DHS toward emerging trends and cybersecurity threats.

Adversarial forces such as China and Russia demand greater control of their cybersecurity environments and limit openness in communications. Such divergent approaches create a continuous challenge for an open society such as the United States, where democracy and free speech ideals exist. By contrast, to sustain massive oversight and censorship, China employs more people to monitor cybersecurity and intrusion than those who serve in the country's military forces. Foreign intrusive forces are part of the greater conflict in cyberspace, as witnessed with the Russian hacking of political campaigns during the 2016 U.S. presidential election, attempting to weaponize information to their advantage. The Colonial Pipeline attack was purportedly carried about by a ransomware group called the DarkSide, which is based in Russia or possibly elsewhere in the former Soviet Union.

Since 9/11, numerous administrations and Congress have stressed the critical importance of public-private partnerships to make the nation safer against attacks including cyber. This has not become the intended reality largely because the private sector's capabilities, assets, and intentions needed to avoid future cyberattacks have not been adequately addressed. Advanced integration of the private sector energy entities

should include all phases of disaster management and be integrated in public-private partnerships as part of DHS security policy creating a more robust public-private partnership endeavor.

Repeatedly, presidential administrations and Congress have not made the private sector security a top priority and have taken a hands-off approach with the thought that market forces would encourage levels of security sufficient to address modern security threats. Some barriers to forming a better partnership have been the lack of information sharing, mistrust, and misinformation. This crisis needs to be urgently addressed because government and law enforcement entities possess critical threat assessment knowledge that can be shared with private entity partners. Sharing knowledge through the engagement of law enforcement agencies such as the Federal Bureau of Investigation (FBI) and the United States Secret Service can effectively deter, disrupt, and help to prevent future cyberthreats. Law enforcement can work diligently with private industry to assist in the apprehension of cybercriminals through notification and help secure networks and vulnerability mitigation. A partnership with law enforcement would help the private sector confront the challenges created by technical barriers such as encryption technologies, which are needed to gather time-sensitive information.

As a result of recent cyberattacks, President Biden signed a national security memorandum on 28 July 2021 to significantly improve critical infrastructure systems and cybersecurity guidelines. The National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems concludes that the systems communities depend upon, which are often private entities, are becoming more vulnerable. Critical energy systems are interconnected in nature, and a major disaster might be hard to recover from as there could be significant outages cascading into multiple critical sectors. Attacks on privately owned older industrial control systems (ICS) and their respective operations technology (OT) have the potential to create enormous physical damage and create a danger to human lives. This risk is increasing as private company ICSs were historically designed for reliability and safe operations but not necessarily for cybersecurity, and many of these systems predate the internet. Not long ago, ICS and other OT devices were used in isolation, and information technology (IT) professionals did not worry about security as the systems were closed off from traditional IT networks. However, today the OT and IT networks have converged, and there are increased cybersecurity risks.

Energy pipelines appear to be an area of great opportunity targeted by hackers, and there is concern that oil and gas companies are ill-prepared to withstand major attacks. Large networks of power plants, electric grids, and energy pipelines in the U.S. remain highly vulnerable to continued cyberattacks, according to Chris Krebs, the former director of the DHS Cybersecurity and Infrastructure Security Agency (DHS CISA). The increase in recent attacks shows that energy organizations continue to experience a large and disproportionate series of attacks compared to other industries such as transportation and health care.

To further enhance CISA's effort, the CISA Cybersecurity Advisory Committee was established in June 2021 as a collaborative board comprised of industry, state, local, tribal, and territorial government leaders. This board brings together subject matter experts from critical infrastructure sectors and the needed exchange between public and private cybersecurity partnerships. CISA has also created the Cyber Awareness Program as a national public awareness effort to increase the understanding of cyberthreats with the goal to use social media platforms to help both public and private partners combat ransomware attacks.

Within the realm of cybersecurity, the United States operates in many disconnected and disparate silos. There needs to be a more centralized approach.

On the legislative front, a necessary CISA cyber-incident reporting requirement was defeated in the compromise fiscal year 2022 National Defense Authorization Act (NDAA) on 7 December 2021. The failure of this requirement set back a major bipartisan effort to have critical infrastructure operators report cyberattacks to the government through a CISA 72-hour cyber-incident reporting requirement for companies operating within the 16 U.S. critical infrastructure sectors. Although specific provisions were not included in the 2022 NDAA, the bill authorized CISA to establish a National Cyber Exercise Program to simulate a complete or partial shutdown of critical infrastructure networks by a cyber incident. The bill also gives DHS the authority to enter into voluntary public-private partnerships with internet ecosystem entities to detect malicious cyber actors.

Congress also needs legislative initiatives to force private companies to adhere to specific cybersecurity standards. Currently, electric utilities are further ahead in preventing and preparing for cyberattacks than the oil and gas industries. Renewed congressional pressure on all private entities could mandate minimum cybersecurity standards. However, there remains a roadblock by industry lobbyists who prefer to hinder such efforts due to the inherent costs and added burdens placed upon private sector energy-providing businesses. Nonetheless, there is an urgent need to work collaboratively with the private sector to implement greater controls to avoid the ever-increasing cybersecurity problems as 85% of critical energy infrastructure suppliers are in the private sector with many being small businesses. These companies can be more vulnerable to cyberattacks because they frequently have less resources dedicated to cybersecurity than large businesses. In order to address this, the Federal Trade Commission – in concert with DHS, the National Institute of Standards and Technology, and the Small Business Administration – initiated a national education campaign in 2018 to assist small business owners in understanding cyberthreats and how to better protect their businesses (see Figure 1).

Figure1. FTC Launches Initiative on Small Business Cybersecurity (2018).

Impact on Military Operations and Readiness

Experts in the U.S. military have also pointed out how the Colonial Pipeline hack could impact future operations. The U.S. Transportation Command (TRANSCOM) has acknowledged that, although this attack did not directly assault military networks, the event questions the viability and safety of commercial companies and their affiliated networks – a crucial element of the Defense Department's logistics network. TRANSCOM relies on commercial vendors for gas, jet fuel, and the movement of troops and supplies, including sea freight transportation. Without reliable commercial vendors, the military services are limited in their ability to remain supplied and agile. Hacking the supply chain is a constant threat to every military system, making the Department of Defense's cybersecurity challenges even greater. Part of the threat is due to a growing dependence on cloud-based systems and supply chain host databases, which can expand the Pentagon's vulnerabilities and attack surface.

The Need for a Centralized Approach

Within the realm of cybersecurity, the United States operates in many disconnected and disparate silos, and there needs to be a more centralized approach. Government agencies address cyber regulation and threats through the 16 different infrastructure sectors that CISA has identified, which is inefficient and ineffective. Although there are certain specific needs for each individual infrastructure sector, there is also an opportunity to centralize cyber-defense objectives and regulations. Vulnerabilities are often similar across sectors and industries, and a centralized approach could find similar solutions to cyberthreats. Other industrialized democracies have adopted a more centralized approach, such as the Network and Information Security Directive in the European Union. The goal of this directive is to propose uniform cybersecurity standards across industries and among its 27 member nations. Other nations such as Britain, Canada, and Australia have also moved in this direction, consolidating their cybersecurity functions under one agency that can more readily work with the private sector.

Conclusion, Recommendations, and Future Actions Needed

Cyberspace and cybersecurity have become increasingly vulnerable and an active threat to homeland security. Although legislative steps have been taken to improve cybersecurity at the congressional level, there remains a greater sense of urgency on cyber-incident reporting. These steps would take a bipartisan political effort. One solution would be a provision to set a five-year term for the CISA director, giving this agency the needed leadership to move cybersecurity forward. This position is a president-nominated and senate-confirmed agency position and should not be subject to political infighting in Congress. CISA's director position is too important and needs to remain stable through turbulent political times, and interim leaders will diminish this mission. As cyberattacks continue to grow in frequency, CISA must have stable leadership guiding the nation's cyber preparedness.

Another important action requires developing a cyberthreat information collaboration environment within DHS. There is an urgent need to continue developing an integrated and networked approach for collaborative sharing between federal, state, and local governments and the private sector. However, there are multiple barriers, including cultural, organizational, and legal impediments between the various levels of government, private sectors, and nonprofits. At present, these processes operate on an ad-hoc basis. Suggestions include creating a Collaborative Defense and Analysis Centers network at the CISA regional offices and creating a cultural shift to overcome barriers and stovepipes hindering the collaboration and sharing needed to streamline interagency processes.

In summary, cybersecurity is a national security imperative. Cyber activities are part of a network spread approach, whether perpetrated by nation-state actors or criminal enterprises. The network spread concept is now more applicable to the threat versus a traditional time-bound homeland security approach and, therefore, reactive emergency management responses do not work today. Instead, a systematic, sustained, and concerted network approach is necessary to address the growing cybersecurity threats and the needed public-private collaborative defense and threat sharing efforts in the cyber domain.

Chandler Lofland is currently a graduate student at Post University Master's Degree Program in Public Administration with a concentration in Emergency Management and Homeland Security. Graduate of the University of Connecticut with a degree in General Studies, Magna Cum Laude. He will pursue employment in a government agency upon graduation in Fall 2022.

Raymond (Ray) Walker has over 44 years of experience leading and managing complex, multidisciplinary, and highly sensitive programs within the Department of Defense and other federal agencies. Throughout his working life, he has served with distinction as a U.S. Marine Corps Officer, federal employee with the Central Intelligence Agency (CIA), and as a supporting contractor with the Departments of Defense, Justice, State, and Homeland Security. Many of the programs he managed throughout his career range in breadth and scope from strategic level/worldwide systems to special use applications of science and technology. He earned undergraduate degrees in Political Science and Business Management from Salve Regina University in Newport, Rhode Island, a Master's in Business Administration from Chaminade University of Honolulu, Hawaii, and executive level certifications as a Chief Information Officer from the University of Maryland and the U.S. General Services Administration in Washington, DC. He currently teaches online undergraduate and graduate level courses in the Emergency Management & Homeland Security program with Post University, located in Waterbury Connecticut.

INTERNATIONAL
HAZARDOUS
MATERIALS RESPONSE TEAMS
International Association of Fire Chiefs

Preconference: June 8, 2022
Conference: June 9 - 12, 2022
Hilton Baltimore | Baltimore, MD

IS YOUR DEPARTMENT PREPARED FOR

THE UNEXPECTED?

For over 30 years the **International Hazardous Materials Response Teams Conference** has offered informative sessions and unique hands-on training designed to tackle the most pressing hazmat issues at all levels of experience.

WHAT TO EXPECT

This four-day event offers attendees hands-on training across a range of essential topics, including:

- Biothreat response & sample collection
- Incident management best practices
- Chemical & physical properties of hazardous materials
- Recognizing & responding to commercial explosive incidents

Learn more and register today at:
IAFC.org/HazmatConf

EXHIBITORS

Bring back the newest hazmat gear for your department, with more than 100 exhibitors showcasing the latest innovations in the hazmat industry.

CONNECT WITH US
#Hazmat2022
@IAFC @firechiefs @IAFC

POWERED BY:

Best Practice: Auxiliary Radios for Healthcare Facilities

By Ashleigh Holmes

Although power outages may be a nuisance, recent disasters have proven that communication redundancies are paramount, especially for critical care facilities that assist older adult populations, such as hospitals, retirement homes, and rehabilitation centers. The New York City (NYC) Emergency Management Department's emergency radio communications program fulfills that need.

Updating an Established Communications Program

Established in 2014, this program continues to serve as an auxiliary line of communication for area healthcare facilities. The program is mutually beneficial. Not only does it provide an additional means for critical care facilities to communicate with NYC Emergency Management when first lines of defense (i.e., communication pathways such as landlines, cell service, texting, and internet) are compromised or inoperable, it also allows NYC Emergency Management to provide participants with situational awareness during emergencies.

In 2021, the New York City Department of Information and Technology Telecommunications (DoITT) upgraded its equipment and programming of the NYC DoITT Citywide Radio Network with a new operating system to better streamline communication and alleviate radio traffic. The program's goal is to ensure that the facilities' equipment is compatible and compliant before switching over to the new system. NYC Emergency Management's health and medical unit, which oversees the program, has been working steadfastly to confirm radios are compatible with the newly established network by swapping out or reprogramming the provided equipment.

Approximately 320 radios were issued to hospitals, nursing homes, adult care facilities, and the New York Blood Center. The equipment includes the APX 4000 handheld portable radio, the APX 4500 base station radio, or the consolette radio APX 8500 with the MCD 5000 desk set. Equipment issuance depends mainly on transmit ability. The day-to-day operation and maintenance are also conducted by the health and medical unit.

How It Works

Participating organizations receive radio equipment and are trained in radio operations and etiquette. The facilities can then communicate with NYC Emergency Management's 24/7 operations center, known as Watch Command. Watch Command monitors citywide radio frequencies as well as local, national, and international media and weather. There are currently 276 participating partners in the program across the five boroughs of New York City, and that number continues to grow.

"The emergency radio communications program is a lifeline connecting us to help at any time. It's important to know we aren't alone out there," said Queens Nassau

NYC Emergency Management health and medical specialist Maurice Zuniga advises an adult care facility staff member on radio maintenance in Queens, NY (Source: NYC Emergency Management, 2022).

Rehabilitation and Nursing Center Administrator Joshua Teitelbaum in a personal interview conducted on March 10, 2022. "I can't stress enough how vital it is for us to have this program as part of our emergency preparedness and to be partnered with NYC Emergency Management who can advise and offer valuable resources and aid to us at a click of a radio button. It has been a great education and in-service opportunity for our staff in participating in all the monthly drills."

"At The Silvercrest Center, the emergency radio communications program prepares us for crisis management before it occurs. Crises occur when they're least expected. Thus, a communication plan is a part of disaster preparedness," said Dr. William Palumbo, vice president and chief operating officer at The Silvercrest Center for Nursing and Rehabilitation, in a personal interview conducted on March 11, 2022. "Having a crisis communication plan is a necessity for each long-term care facility to have before one happens. Attending the [program] exercises ensure us at The Silvercrest Center that we are ready."

Although there is no cost to participate in the program, a set of standards and responsibilities outlined in the Memorandum of Understanding (MOU) must be adhered to. The MOU is signed by the receiving facility before installation. Healthcare facilities interested in participating in the program can contact NYC Emergency Management.

"The emergency radio communications program is a tool in the emergency management toolbox. It serves as another source of emergency communications when all other communication types have failed," said New York City Emergency Management Health and Medical Specialist Maurice Zuniga, in a personal interview conducted on March 10, 2022. "I liken its availability to a fire extinguisher: always available but only used when [it is] really, really needed."

Ashleigh Holmes is the community and ethnic media relations senior press officer at the New York City Emergency Management Department, where she has responded to various emergencies. She assists the press team in day-to-day press operations and serves as one of the agency's spokespersons, helping to develop and distribute information to the news media. Before joining NYC Emergency Management, she worked in television news for over 10 years at WHDH-TV in Boston, MA.

Watch commander conducting roll call with healthcare facilities at NYC Emergency Management's Emergency Operations Center in Brooklyn, NY (Source: NYC Emergency Management, 2022).

A Foot in the Door – The Value of Internships

By Sambavi Jani

Experience required. Many jobs require wide-ranging qualifications and expertise to be able to apply and interview. However, people often ask, "How can I get the experience if I cannot get a job?" A great way to get "a foot in the door" is through internships, which can be vital in the emergency management field. Multifaceted and sometimes fast-paced, this is the type of profession where one must have the drive and passion for helping others and serving the community. Despite some public misconceptions that emergency management is only active during an event (which is often the only time an agency receives media attention), it is a 24-hour-a-day, 7-days-a-week, 365-days-a-year profession. Therefore, exposure to what happens in the field on "blue sky days" and during an emergency or disaster is paramount for someone new to the profession to experience.

An internship can expose someone to all phases of emergency management, effectively showing their strengths and weaknesses. For instance, after providing training, some may realize that public speaking is not for them. If that is the case, they can try other roles within the profession that better suit their needs and personalities. It is essential for this type of profession to learn how an agency or organization operates and how a community responds during a critical event. During an event, one can see the systems and methods used to accomplish a mission. One can also see how each agency integrates behind the scenes in the emergency operations center. Many emergency management professionals enter the field after witnessing or participating in an actual event, such as Hurricane Katrina or the terrorist attacks of 9/11.

Advantages of an Internship

Paid or unpaid, there are many advantages to participating in an internship. According to a 2020 article by Indeed, benefits include but are not limited to job experience, research experience, exposure to various tasks and departments, mentorship, building a resume, building confidence, and transitioning to a permanent job. Specifically, in emergency management, having different tasks and working with other units can help people develop the skills needed to manage the many functions that emergency managers perform. As noted in the article, some internships can also become full-time positions. In a recent study by the National Association of Colleges and Employers (NACE), 66.4% of eligible interns received full-time positions after the program ended in 2020. Whereas, in 2019 only 43.7% of students got a job offer without completing an internship program according to CompareCamp.

Challenges of an Internship During a Global Pandemic Repsonse

No internship is perfect, and there will be some limitations and challenges and the past two years were no exception. The COVID-19 pandemic shattered the job market and forced many companies to work remotely. Due to the hands-on nature of internships, COVID-19 impacted

the effectiveness of a program once it went virtual. In the same study mentioned above by the NACE, in 2020, 72% of summer internships were virtual, and the quality of interactions and networking with the interns were hindered. A study by the Center for Research on College-Workforce Transitions (CCWT) found that, in 2021, only 22% of students participated in an internship, and one in five students split time between in-person and online positions.

Another challenge caused by the pandemic is that internships became very competitive due to virtual or shortened time frames. In an article by CNBC, the author noted that a student who applied for a couple of internships never received a reply from the employer or heard they had canceled the program. As a result, internships became competitive because the number of applicants outpaced the availability of programs. In addition to being competitive, one student found it difficult to stay motivated to apply for internships due to companies' lack of responses.

Below is a specific example of how COVID affected the networking process. Andrew Wasserman participated in New York City's (NYC) John D. Solomon Fellowship for Public Service in 2020. He noted during a personal interview on 11 March 2022 that, although his placement with NYC Department of Environmental Protection was in-person, he found it difficult to meet and network with the other Solomon fellows who were part of his cohort. In addition, Wasserman mentioned the fellowship did not host events like they had in previous years such as the Solomon Family Dinner event, where members of the current fellowship class can meet and connect with any alumni and mentors who participated in the fellowship in previous years.

Wasserman wished networking with others happened in a more organic way rather than over Zoom and social media. He felt that he would have been able to interact with fellow participants more effectively if the program was fully in-person. Although he experienced some challenges, Wasserman noted he had a very positive experience during his time with the fellowship and he was able to perform tasks in the field. In addition, he was hired by New York City Emergency Management a few months after his fellowship ended

Best Practices for Interns

The value of internships and fellowships is immeasurable when considering the amount of experience gained while employed. Another significant factor in emergency management is networking and building relationships. A 2018 case study about internships notes that relationships can open doors to other internships and employment opportunities. For example, if a position is not available after completing the internship, the intern's advisor may know if another agency or organization has open positions. Additionally, people who decide to opt into different career paths, an internship can confirm whether or not they are passionate about the field they are interning for.

Other best practices for interns according to Columbia University's Center for Career Education include but are not limited to:

- Meet coworkers – By trying to meet each person, the intern can continuously build relationships during the program. Coworkers can also be valuable resources when the advisor is not available to answer questions. As companies decide to keep a remote schedule or a hybrid schedule, it may seem difficult to meet coworkers. One suggestion is to reach out to one person who said something interesting at a meeting and ask them to meet one-on-one to discuss the topic in more detail. Another suggestion is to ask for a mentor for the duration of the program to assist in any issues that may arise. This also provides valuable network building opportunities.
- Set goals – Setting goals helps set expectations for the intern and the advisor.
- Watch and learn – Being observant can provide an understanding of the organization's culture and the people. It is also essential to ask questions as they arise, which demonstrates a willingness to learn.
- Be professional – It is imperative that interns present themselves professionally each day to show they are serious about working there.
- Develop time management – Time management of projects and keeping track of deadlines are critical skills that some people struggle with, but they are essential for staying organized

With these tips in mind, an intern will have the best possible internship experience.

Not Just for Students

Internships are not and should not be exclusively available to students. They should be open to working professionals looking for career changes or expanding their skill sets. For

instance, if a member of the American Red Cross's (ARC) Disaster Action Team (DAT) who has responded in the field wants to learn what happens behind the scenes, an intern program can provide some experience with interagency coordination. Another example in which internships can benefit working professionals is if they were, unfortunately, let go. Looking for another job can often be a daunting and challenging task. An internship may be the best way to ease back into the job market and make new connections.

Even if a person has some emergency management experience, there are other aspects of the profession that can be explored and shown differently through internships. In addition, the daily interactions with different disciplines may introduce other interdisciplinary areas to explore, such as healthcare emergency management. For emergency management to grow, there must be a way to increase the availability and visibility of internships and fellowships. By opening internships to all interested in new opportunities and not limiting them to students in undergraduate or graduate programs, the field can continue to evolve and grow.

Sambavi "Sam" Jani is an emergency management specialist with the New Jersey Department of Children and Families, Office of Emergency Management. Her emergency management career spans government entities and the private sector. She began her career with Hurricane Sandy in 2012. Since then, she has had the opportunity to work at the state and local levels in planning and responding to various events. She has found her passion lies with the importance of preparedness, training, and exercises. She participated in NYC's John D. Solomon Fellowship for Public Service. She holds a Masters in Professional Studies in Emergency & Disaster Management from Georgetown University. She is also a member of International Association of Emergency Managers (IAEM) Region 2 and has earned the designation of a Certified Emergency Manager.