ONE STEP AHEAD

Spring 2023

Insights of the

INSTITUTE FOR HOMELAND SECURITY

SAM HOUSTON STATE UNIVERSITY®

Message from the Editor/Director

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY®

Partners,

On behalf of the team here at IHS, I am pleased to present the inaugural edition of the following publication:

SHSU - Institute for Homeland Security

- One Step Ahead -

A Critical Infrastructure Protection Research and Strategy Publication of Insights

This publication of insights is a collection of research completed on behalf of IHS by our partner scholars, practitioners, and faculty members. These papers are a representation of our Core Purpose: We Stay One Step Ahead, transforming knowledge to protect critical infrastructure. Since our inception in September 2021, we collaborated with private and public professionals operating in the critical infrastructure protection (CIP) space to create innovative, value-added knowledge tailed to the needs of our constituents supporting Texans and the nation's economy. These research papers cover a broad spectrum of CIP topics, and it is our hope that the information herein complements to complete research gaps in the CI protection space. This publication of insights is a step for us to build a trusted network that connects homeland security professionals.

We are always on the lookout for research topics and projects. There are two ways to partner with us. First, if you work in any of the CIP sectors and have a research topic that can add to the CIP knowledge base. Please send an email to ihs@shsu.edu with your idea. Second, if you are interested in submitting and conducting research, go to our website at www.ihsonline.org and select Research. From there, navigate to the Research Proposal tab and submit a proposal. Our team will review your submission and provide feedback.

Thank you for being part of our goal to stay **One Step Ahead**!

Sincerely,

Michael J. Aspland
Executive Director

ONE STEP AHEAD

Editorial Office:
Institute for Homeland Security
Criminal Justice Center
Sam Houston State University
PO Box 2296
Huntsville, TX 77340
Email: IHS@ihsonline.org
www.ihsonline.org

Legislative Intent

Enhance the security and resilience of the transportation, energy, chemical, and healthcare sectors for Texans and the Texas economy.

Four Pillars

Texas Nexus

We believe in a secure and unified Texas, connecting our private industry partners with public institutions through productive conversation.

One Step Ahead

Our focus is to stay ahead in an ever-changing security environment by providing innovative solutions that support business continuity and critical infrastructure protection.

Complement to Complete

We aim to fill the gaps and meet the needs of critical infrastructure sectors alongside our institutional partners.

Disruptive but Helpful

We believe in serving our private industry partners and public institutions in ways not done before.

Priorities

Priority 1:

Deliver training, education, and industry-focused research solutions.

Priority 2:

Build a trusted network that connects homeland security stakeholders.

Priority 3:

Establish an organizational structure to align resources and ensure sustained success.

Research at IHS: The 30,000 foot view

By now many of you have come to know that the Institute for Homeland Security at Sam Houston State University is a valuable resource for research on current topics critical infrastructure protection. Here, I will guide you through our process for uncovering industries most vexing questions and matching them with research partners to provide applicable current solutions for our readers.

Currently our research interests are driven by seven critical concepts that have emerged through our continuing relationships with government and industry partners. These items (listed below) are the first iteration of IHS Critical Concepts. Yet we know that as the security environment continues to evolve, so will our view of critical concepts.

- Workplace Violence: Exploring detection and prevention methodology that is teachable to security practitioners and company personnel at large, that meets operational, compliance, legal, medical, law enforcement and security management regulatory standards.
- Supply Chain Risks: Identifying best practices for efficiently and meaningfully assessing critical infrastructure corporations vulnerable supply chain interdependencies to determine 1) how to effectively quantify crisis management readiness by key suppliers such that 2) critical infrastructure corporations can make strategic choices using identified risks in decision making.
- Security Drone and Robot Deployment: Assessing the cost effectiveness of security drones and security robots as part of government approved security management for: access control, visitor management, cargo inspection, perimeter patrol, loss of containment detection, occupational safety management and emergency management (e.g., firefighting, enclosed space rescue, toxic release containment, at-height emergency maintenance).
- Mass casualty Response: Benchmarking best practices for hospitals and medical centers in Texas to identify more effective teams, processes, and staffing products, responding to a mass casualty event.
- Cyber-Security Threat: Benchmarking best practices in responding to a cyber-security threat at hospitals and medical centers in Texas, including attacks (e.g., ransomware), or accidental breaches involving a loss of protected data or interruption of critical operating systems which degrades operating capabilities.
- Social Network Analysis (SNA): Broadly, using a SNA approach to identify organizational personnel and staffing decisions and explore the viability of that address how private and public organizations could modify structure and processes more effective teams, processes, and staffing products, while maintaining workforce and production compliances.
- Process Safety: Assessment of whether or not, and how, process safety countermeasures can be incorporated into USG approved security management programs for access control and intrusion detection purposes.

Moving forward it is our goal to grow and evolve our Critical Concepts around the needs of our industry and government partners. Your contacts at IHS will always be listening to your concerns about critical infrastructure protection and strategy.
What do you do if you want to publish with IHS? Use the research tab on our website (IHSOnline.org) to find the proposal submission form. This form was designed to be fillable and conveniently attachable to an auto populated e-mail address (IHS@shsu.edu).

We continuously receive and fund projects that address our critical concepts. Our research team meets weekly to review submissions, contact potential authors, and build our research library.
Thank you, and we look forward to staying one step ahead,

Ryan Randa PhD
Research Director
Institute for Homeland Security

Contents

MH Peer Support in Civilian Businesses

Zeno Franco, PhD
Prepared for Sam Houston State University

Executive Summary

In developing a strategy for assisting Texas businesses to identify and respond to potential mental health crises in employees, peer support strategies offer an important, low-cost option. Fellow employees are often better positioned to observe MH symptoms and related behaviors than supervisors or EAP professionals. Peer-to-peer support is often better tolerated and viewed as less intrusive than formal MH intervention. Well trained employee peer mentors can provide basic psychoeducational interventions about a range of issues, be trained to identify indicators of more serious MH problems including the potential for workplace violence, and can refer fellow employees to more comprehensive services when needed.

- Peer-support models have been shown to help reduce PTSD symptoms which can include violence and suicidal ideation. Peer support strategies developed with this complex population can help inform a wide range of work-place based peer mentor programs.
- Small businesses can leverage peer to peer support to identify high risk behaviors
- Large businesses may be able to use a combination of peer support and automated approaches to identify high risk behaviors
- Privacy and ethical concerns will be important considerations

Background

Mental health peer support as a para-professional led intervention is an important alterative to licensed mental health care for a number of reasons. These include increased acceptability from individuals who may be warry of seeking professional care, larger number of individuals available for this type of work than licensed professionals, and the ability for peer mentors to connect in a way that is based on similarity of social position. Further, in places of work, networks of co-workers who are familiar with an individual may be well placed to detect impending MH crisis and intervene early [1], thus reducing burden for both the individual at risk and for the employer [2, 3]. Given current labor shortages and increased focus on inclusion, increased focus on employer driven programs to enable individuals suffering from serious mental illness to be employed is also a significant consideration in workplace embedded peer-to-peer mental health peer support [4, 5].

As workplace violence becomes more commonplace, MH peer mentors may also be able to identify and flag employees who are disaffected or have a specific grievance that might escalate. While there are serious privacy and ethical concerns that have to be addressed, peer mentors may be uniquely positioned to head-off workplace violence by working through issues with at risk employees as a first step, and reporting concerns if a specific threat becomes apparent.

Training for workplace MH peer mentors, individuals existing aptitude for this work, developing reporting and referral frameworks and addressing privacy, HR, legal and risk management consid-

erations are all areas for serious inquiry. Training considerations become particularly important in larger scale workplace settings as the intention and value of MH peer mentorship interventions could be lost without attention to fidelity to the model.

Despite the complexity of this domain, workplace based MH peer support can be flexibly applied to multiple MH conditions. Leveraging technology, including interactive digital platforms and smartphone applications designed to support peer mentors to become more adept in this role may enable scaling large corporate scenarios.

Problems

Privacy considerations are paramount in multiple populations we have worked with using MH peer mentorship. For example US military veterans and first responders are concerned about keeping information about their mental health status confidential – particularly as it relates to their employers. This is primarily due to these populations running the risk of being removed from active duty or deployable status in the event they receive certain types of MH diagnoses. Rules and guidance for in house peer mentors around appropriate privacy is important, but may be difficult to negotiate, particularly if the employee and the peer mentor are within the same reporting structure.

To mitigate privacy concerns, some strategies might include systematically ensuring that MH peers in the workplace come from different units with different reporting structures as compared to the employees they are working with. Technology solutions, including training and real-time support tools like peer mentor smartphone applications could provide just-in-time guidance about privacy and confidentiality, as well as scenario-based practice opportunities.

Further, clear guidance and transparency about situations that require peer mentors to breach confidentiality should be made, focusing specifically on universally accepted reportable events of threat to self, threat to other, child abuse or elder abuse. However, as an employee becomes more at risk, their willingness to disclose usually decreases, and understanding of the risks of being reported for clear threat targets increases. Peer mentors should also be trained to observe employee behaviors to identify potential problems before they boil over

Workplace peer support focused on prevention of violence may specifically look at scenarios where an employee has a grievance that seems unresolved. It is important to recognize that some of these grievances may be for cause, and that the employer or the work environment has failed to provide redress and resolution. Peer mentors will need a range of referral options and to be fully trained to select the most appropriate referral, which in addition to EAP or HR for some scenarios, might also include referral to an ombuds or Chief People Officer.

Current State of the Art

A range of employee peer assistance programs (PAPs) or member assistance programs (MAPs) have been explored over decades as a strategy for voluntary mutual assistance in organizations and provide a framework for considering implementation considerations for mental health peer support more specifically [6]. Peer referral process have been used in conjunction with Employee Assistance Programs and employee union support systems [7], using peer helpers to identify and provide guidance to employees exhibiting signs of alcohol abuse [8], employee-to-employee substance use and early intervention [9]. Appropriateness of strategies for employee peer support may vary by age of workers, and employers should pay careful attention to addressing the needs of younger, middle aged, older, and mixed-age teams [10]. Further, there is some evidence that different peer strategies for gender and ethnicity may improve acceptability and outcomes [11]. In our work in Wisconsin with US military veterans and mental health peer support for example, the

non-profit partner we work with attempts to match female veterans seeking peer support services with trained female peer support specialist, and to a lesser degree, when possible the agency tries to match or other characteristics such as military service period and/or ethnicity.

There is increased focus on using technology to support peer-to-peer mental health interventions, which can assist specifically in employment based programs with training, information on boundary setting and privacy, as well as providing current referral resources. Technology based systems, including web and smartphone technology can also assist with brief screening for changes in mental health symptoms. This information can be used to alert peer mentors to check-in with their mentee more frequently or to suggest more targeted intervention strategies. For more serious situations, where the employee is struggling with mental health concerns that may impact their employability, crisis alerting strategies that provide just-in-time information to an EAP counselor or similar professional may be a consideration.

Future Solutions

We have been working in Wisconsin with machine learning strategies to identify early indicators of mental health crisis using a Battle Peer (www.battlepeer.com). Working with computer scientists at Marquette University, we have identified a handful of early warning signs specific to US military veterans suffering from PTSD. Creating large, employer driven data sets from technology supported peer support would allow for complex machine learning strategies to be applied to isolate similar warning signs from a general (non-veteran) population in the workplace. Along with these strategies, increasingly sophisticated peer mentor decision support tools could be developed, for example providing brief video based training based on the warning signs from an employee they are working with. Interventions tailored to the specific mental health problem, employee context, and coping styles of the individual would likely provide substantial improvement compared to more routinized interventions based on evidence from treatment selection studies in other mental healthcare models. These more sophisticated, algorithmically driven approaches may facilitate better management of mental health considerations for large employers. For example, even with individual privacy concerns addressed, aggregated anonymized data from peer mental health support systems would show trends in issues that need to be addressed more comprehensively or identify work locations with high incidences of mental health problems.

References

C.W. Wilkinson, Violence prevention at work: A business perspective, American journal of preventive medicine 20(2) (2001) 155-160.

K. Petrie, S. Joyce, L. Tan, M. Henderson, A. Johnson, H. Nguyen, M. Modini, M. Groth, N. Glozier, S.B. Harvey, A framework to create more mentally healthy workplaces: a viewpoint, Australian & New Zealand Journal of Psychiatry 52(1) (2018) 15-23.

B. Agarwal, S.K. Brooks, N. Greenberg, The role of peer support in managing occupational stress: A qualitative study of the sustaining resilience at work intervention, Workplace Health & Safety 68(2) (2020) 57-64.

J. Delman, L. Kovich, S. Burke, K. Martone, The promise of demand side employer-based strategies to increase employment rates for people living with serious mental illnesses, Psychiatric Rehabilitation Journal 40(2) (2017) 179.

J. Cameron, C. Walker, A. Hart, G. Sadlo, I. Haslam, Supporting workers with mental health problems to retain employment: Users' experiences of a UK job retention project, Work 42(4) (2012) 461-471.

M. Golan, Y. Bacharach, P. Bamberger, Peer assistance programs in the workplace, Contemporary occupational health psychology: Global perspectives on research and practice 1 (2010) 169-187.

P. Bamberger, W.J. Sonnenstuhl, Peer referral networks and utilization of a union-based EAP, Journal of Drug Issues 25(2) (1995) 291-312.

P.M. Roman, T.C. Blum, The workplace and alcohol problem prevention, Alcohol Research & Health 26(1) (2002) 49.
R.S. Spicer, T.R. Miller, Impact of a workplace peer-focused substance abuse prevention and early intervention program, Alcoholism: Clinical and Experimental Research 29(4) (2005) 609-611.
R. Spicer, T. Miller, E. Zaloshnja, Substance abuse prevention for the young workforce in the railroad industry: An adaptation of the prevent program, Young Adults in the Workplace: A Multisite Initiative of Substance Use Prevention Programs (2011) 29.
G.M. Ames, L.-A. Rebhun, Women, alcohol and work: Interactions of gender, ethnicity and occupational culture, Social Science & Medicine 43(11) (1996) 1649-1663.

Suggested citation: Franco, Z. (2023). MH Peer Support in Civilian Businesses. *One Step Ahead,* April 2023, 1-4.

PUBLIC AND PRIVATE COLLABORATION DURING AND AFTER WINTER STORM URI: LESSONS FOR IMPROVEMENT AND SUCCESS

David A. McEntire, PhD

Abstract

This technical report illustrates that the private sector performs critical roles in disasters, and reiterates that its collaboration with the public sector is necessary when extreme events occur. Using the February 2021 Winter Storm Uri as a case study, this paper explores the negative impact of the loss of power and subsequent cascading effects. It also reveals numerous areas where the businesses and the government collaborated to meet pressing disaster needs. The implication is that the private and public sectors must increase communication and mutual support when disasters take place.

Introduction and Overview

There is a growing recognition that the "whole community" must be involved in disasters, whether that is to mitigate hazards or be prepared for improved response and recovery operations in their aftermath (FEMA 2011). Businesses are a significant part of this whole community. And one of the most important relationships which facilitates the whole community approach is collaboration between the private and public sectors.

Research reveals that businesses perform important roles before and after disasters occur (Weber, McEntire and Robinson 2002). For instance, the private sector provides donations and volunteers, insures disaster losses, complies with occupational health and safety, plans for transportation accidents, assists with emergency medical care, facilitates sheltering, disseminates warnings and public information, engages in business continuity, and serves as vendors of goods and services.

The aftermath of the 9/11 is a great case in point. The private sector illustrated its value in this anthropogenic disaster and worked closely with the public sector to address significant challenges that were made manifest when the worse terrorist attack occurred in U.S. history. The private sector communicated and coordinated with the government to:

1. Warn and evacuate occupants of the twin towers at the World Trade Center complex.
2. Relocate New York City's Emergency Operations Center and equip it with office equipment and phone lines.
3. Clean up debris generated by the collapsed buildings at ground zero.
4. Set up fences around ground zero for perimeter control.
5. Provide additional site security.
6. Deliver logistical support for Urban Search and Rescue teams.

7. Care for the medical needs of the victims of this horrific incident.
8. Disseminate information to the public through the media.
9. Repair communications and electrical infrastructure.
10. Restore nearby buildings that were damaged as a result of the collapse.
11. Share sanitation services with first responders and recovery personnel.
12. Relocate businesses and resume normal operations.
13. Distribute funds for disaster victims and cover insurance losses.
14. Manage other donations going to first responders and victims of the incident.
15. Replace fire apparatus lost on 9/11.
16. Install fixed, retractable, and removable bollards in front of government buildings to prevent further terrorist attacks.

The following technical report follows up on this prior research, and explores challenges encountered by the private sector and government officials during Winter Storm Uri in Texas in February 2021. It also shares notable successes resulting from this important collaboration.

Problem Statement and Gap Assessment

Businesses encountered a whole host of problems when Winter Storm Uri dumped snow and ice on virtually the entire state of Texas and plummeted temperatures to historic freezing records.

The most obvious challenge was the loss of natural gas and electrical service, and this may be traced – at least in part – to the 1935 Federal Power Act which deregulated electricity in Texas. Later on (in 1970), the Electric Reliability Council of Texas (ERCOT) was created to manage its standards and operating procedures. This resulted in the Texas power grid being a standalone and unstandardized grid. Unfortunately, several weaknesses were revealed in the grid and numerous recommendations were given to remedy the situation. This counsel included three major reports that stressed the need to improve power generation and distribution during severe weather:

- Outages and Curtailments During the Southwest Colder Weather Events on February 1- 5, 2011. (Federal Energy Regulatory Commission & North American Electric Reliability Corporation 2011).
- Extreme Weather Preparedness Best Practices. (Quanta Technology 2012).
- Eye of the Storm: Report of the Governor's Commission to Rebuild Texas. (Sharp 2018).

Unfortunately, as one emergency manager commented, "many of these recommendations were not followed… which left the electrical grid susceptible to extreme temperatures and high demand." Specifically, the freezing temperatures and weak infrastructure caused the gas lines that provide power to the electricity companies to become semi-frozen in the pipes. In fact, some estimates suggest that half of the gas supply was hindered during the storm (Communications Team, 2022). Many plants shut down as a result, which prevented the generation and distribution of electricity.

Meanwhile, the demand for power was increasing because individuals, families, businesses, and government entities were striving to keep their buildings warm and habitable. The combination of a limited supply of electricity and heightened demand created a situation where rolling blackouts would be needed to prevent a total failure of the system. This loss of power forced many businesses to shut down relevant operations (e.g., extraction, manufacturing, distribution, sales, etc.).

A closely related problem was the provision of incorrect or insufficient Information about the generation and transmission of electricity. When Winter Storm Uri made its way to Texas, ERCOT advised government leaders and the media that rolling blackouts would be needed to maintain partial operation of the grid. ERCOT notified businesses and citizens that power would be cut on a rotating basis in each power grid for approximately 30 to 60 minutes.

Unfortunately, this announcement appears to have been erroneous. Some locations never lost power, but power was turned off in many locations of Texas for hours and even days on end.

This resulted in the freezing and breaking of pipes and water mains, which subsequently produced flooding in and outside of buildings. Making matters worse, ERCOT did not issue many public statements between February 11th and February 17th. Neither the government nor businesses fully understood what was happening with electricity. One person interviewed for this study stated “We were told that there would be a possibility of sporadic outages, but they would be coordinated and no longer than a specified amount of time. And it was supposed to be intermittent.”

The loss of electricity produced rippling effects, that crippled routine business operations. Water soon became inaccessible for human consumption or for manufacturing purposes. Roads became impassible. The supply chain was severely disrupted and needed goods and services were severely curtailed. This included everything from food and water to generators and piping materials.

Although businesses were clearly victims of this extreme weather event, they also demonstrated incredible resilience and worked collaboratively with the government to respond to the challenges they faced. Successes were witnessed in countless areas:

- Businesses received information about the storm from the National Weather Service.
- The private sector helped remove snow and sanded/salted icy roads.
- Over 60 private tow truck operators were called to help clean up a 135-car pileup in Fort Worth Texas.
- Police, fire fighters and other government employees worked with an apartment complex to shut off water and evacuate residents to warmer locations.
- Police officers picked up nurses from their homes and drove them to hospitals so they could fill their shifts.
- Essential employees who were isolated at a chemical refinery walked to a nearby convenience store and relied on this establishment to obtain life-sustaining water and food.
- Government officials moved evacuees and others seeking refuge from the extreme temperatures to hotels in order to avoid congregate sheltering during Covid-19.
- Emergency management personnel called gas stations to determine which ones were open and had enough fuel to supply the needs of emergency vehicles.
- Government agencies contacted retail establishments to acquire water for public distribution and transport companies helped to get water to cities and counties that needed it the most.
- Stores provided generators for government agencies, hospitals, and nursing homes.
- Emergency managers helped access and ship diesel so a local petrochemical plant could keep its generators running and avert a potential leak and explosion.

- Government leaders shared information through private media entities about how to people could protect themselves from the cold (e.g., with layering of clothing, blankets, lining windows, etc.).
- The state acquired fuel from private sector providers and sent it to those in need around the state.
- Government officials were able to operate virtually because of software provided by the private sector (e.g., Microsoft Teams, Zoom).

Topic Discussion

As demonstrated, the private sector encountered many problems related to Winter Storm Uri. In addition, there were countless cases where the private and public sectors worked harmoniously to address pressing disaster challenges. With these issues in mind, there are several areas where the private sector can help to prevent a recurrence of what happened during Winter Storm Uri. And there are a variety of recommendations that can facilitate more effective and efficient public/private interactions in future disasters. Several will be mentioned here:

1. The private sector must be involved in rebuilding and strengthening the power grid in Texas.
2. Businesses are required to repair damaged public infrastructure (e.g., roads and watermains) and flooded homes.
3. Large corporations and small companies must anticipate unlikely hazards and complex disasters and develop or expand contingency plans accordingly (e.g., virtual operations).
4. Private business leaders must increase ties and communications with the National Weather Service as well as ERCOT to better comprehend severe weather and the implications this has on the provision of electricity.
5. Management and labor must augment levels of preparedness by reviewing vendor contracts, stocking needed supplies, and anticipating what orders should be placed in advance when disasters threaten.
6. Corporations and businesses should look for ways to provide essential services after a disaster, whether it be food, water, transportation, sheltering, fuel, generators, etc.

The Way Forward

Research reveals that businesses are essential partners in the whole community approach to disasters. In addition, case like Winter Storm Uri illustrate that the private sector must work closely with government leaders to address issues ranging from the loss of power and information sharing to supply chain issues and the rebuilding of critical infrastructure. By learning from prior disasters and implementing change, businesses can help themselves and the government to be more resilient.

References

Communications Team. (2022). Texas February 2021 Winter Storm: Lessons Learned One Year Later. https://www.deandraper.com/blog/texas-february-2021-winter-storm-lessons-learned- one-year-later.

FEMA. (2011). A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action. FDOC 104-008-1. https://www.fema.gov/sites/default/files/2020-07/whole_community_dec2011_2.pdf.

Federal Energy Regulatory Commission & North American Electric Reliability Corporation. (2011). Report on Outages and Curtailments During the Southwest Cold Weather Events on February 1-5, 2011: Causes and Recommendations (pp. 1-218).

Quanta Technology. (2012). Report on Extreme Weather Preparedness Best Practices. (p. 1-71).

Sharp, J. (Ed.) (2018). Eye of the Storm: Report of the Governor's Commission to Rebuild Texas. (p. 1-168).

Weber, Richard T., McEntire, David A., Robinson, Robie J. (2002). "Public/Private Collaboration in Disaster: Implications from the World Trade Center Terrorist Attacks." Quick Response Report #55. Natural Hazards Research and Applications Information Center. http://www.colorado.edu/hazards/qr/qr155/qr155.html

Suggested citation: McEntire, D.A. (2023). Public and Private Collaboration During and After Winter storm Uri: Lessons for improvement and success. *One Step Ahead,* April 2023, 5-9.

RANSOMWARE PREVENTION AND DEFENSE: A HARDENING GUIDE FOR SMALL AND MEDIUM-SIZED BUSINESSES

Narasimha Shashidhar
Cihan Varol

Introduction and Overview

Small businesses typically don't expend as much time, energy, and resources on cybersecurity and information assurance protocols as large corporations do. To this end, they often fall prey to malware and related cyber-attacks. Ransomware is a specific type of malware that threatens the victim's access to her data unless a ransom is paid. It is also known as a cryptovirus due to its method of operation. Typically, ransomware encrypts the contents of the victim's hard drive thereby rendering it inaccessible to the victim. It might also threaten to publish sensitive data if the victim refuses to pay up. Upon payment of the ransom, the decryption key is released to the victim, with no guarantees that the data will indeed be recovered. This means of attack is therefore also sometimes aptly called cryptoviral extortion. The ransomware itself is delivered to the victim using several channels. The most common channel of delivery is by masquerading the malware as a Trojan horse via an email attachment.

Ransomware is projected to reach $40 billion by 2025 and exhibits a growing trend for cyber extortion - data being held for ransom. A small business involved in finance, healthcare, or online retail, is more likely to be targeted than others, such as a small-sized restaurant. It can be recognized as either crypto-ransomware or locker-ransomware. Locker-ransomware locks up systems and demands a ransom to make the system usable; this type is commonly seen in mobile devices. The focus of this whitepaper will be on crypto-ransomware in which a system is encrypted with an asymmetric or symmetric key and the only method of recovery is to pay a ransom for a decryption tool. With this in mind, we study this issue and put forth a hardening guide for Small to Medium Size Businesses (SMBs) to best defend and thwart such attacks.

How to Use This Whitepaper

Most articles and published reports in the scholarly literature are inaccessible to the average small and medium-sized business proprietor. This is either because the contents of these materials are highly technical, or the solutions presented are time-consuming or prohibitively expensive to deploy. This has motivated us to write this whitepaper in plain English with minimal technical jargon to reach a broad audience. Furthermore, we put forth solutions that are open source and can be deployed effectively with minimal expense and technical expertise. This whitepaper is meant to be read sequentially, from beginning to end. However, the advanced reader may skip to specific sections to best suit their individual needs. This report is accompanied by a descriptive video by the authors that addresses the best industry standards and approaches to take to hard-

en an SMB network and infrastructure from malware, and more specifically the current generation of ransomware.

In addition to proposing hardening defense postures for the SMB, we also develop prevention and mitigation strategies. Lastly, we understand that despite best efforts, some attacks can't be thwarted. To this end, we also propose business continuity and disaster recovery techniques, aimed at getting an SMB back operational and minimizing downtime and lost profits.

Economic Loss

Ransomware costs small and medium-sized businesses more than just economic loss. Forbes reports that a new ransomware attack will be launched every 11 seconds in 2022 and is expected to reach $40 billion by 2025. About 50% of victims end up paying the ransom but are never fully recovered after the incident. The indirect costs which include rebuilding the servers, lost customer base, tarnished reputation, brand erosion, legal costs, regulatory challenges, and lost employee productivity can, in many instances, never be recouped. Thus, a ransomware attack has the potential to devastate small and medium sized businesses. Our hope in this whitepaper is to present tangible techniques and strategies to mitigate this threat.

Most Well-Known Types of Ransomware and Their Modus Operandi

Ransomware and related malware come in many different varieties with as many distinct payloads. Kaspersky[1] identifies the following malware, that have infected both individuals and corporations over the years, to be the most well-known in history:

- Bad Rabbit
- Cryptolocker
- GoldenEye
- Jigsaw
- Locky
- Maze
- NotPetya
- Petya
- Ryuk
- Wannacry

Without loss of generality, most of the ransomware in existence can be classified into two primary categories, based on their modus operandi. While both these classes of ransomware ultimately extort their victims, the subtle difference lies in their degree of data destruction.

a. Denial-based Extortion Ransomware: The primary motivation for the perpetrator in this scenario is to ensure that the victim's computing system remains partially operable. This is so that the victim can continue to interact with the perpetrator with minimal computing functions to pay the ransom. To this end, often the most critical system files and software are left unaffected.

b. Cryptoviral-based Extortion Ransomware: The primary motivation in this instance is to encrypt the victim's drive contents using strong symmetric or asymmetric cryptograph-

1 https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

ic algorithms. In most cases, without payment in a specified time frame, the system is left completely crippled.

StopRansomware.gov[2] is the U.S. Government's official one-stop location for resources to tackle ransomware effectively and contains a wealth of information for SMB.

Common Delivery Vehicles/Mechanisms - Propagating Ransomware

While there are several vectors of attack for ransomware to gain a foothold at an enterprise level, typically the three most common vectors are: a. Phishing and spear phishing email attacks, b. exploiting unpatched software vulnerabilities, and c. trojan horses.

1. Social Engineering Attacks, such as phishing and spear phishing campaigns: Phishing is a form of social-engineering attack designed to trick the recipient into revealing sensitive information. The attack is usually delivered via email and embedded spurious links in an effort to steal credentials, financial information, and other data. Spear phishing is a particularly devious sub-technique of phishing where specific high-profile individuals of an organization are targeted as victims and the emails are custom designed to deceive them into revealing company secrets.
2. Exploit of unpatched software vulnerabilities: Most businesses are dependent upon a slew of software systems and servers for their daily operations. These include operating systems, application software, internet-facing servers, and software daemons with open ports and protocols. Each of these software products needs to be scanned routinely for vulnerabilities and patched in a timely manner.
3. Trojan horses: A Trojan horse, whose name is derived from the Greek story that led to the downfall of the city of Troy, is generally any piece of software that masquerades its true form and disguises itself as a legitimate program. It is generally propagated primarily using social-engineering techniques.

Equipping Small Businesses with Appropriate Defense Strategies

In this section, we discuss some strategies for SMBs to defend themselves against ransomware attacks. In particular, let's look at defense strategies against ransomware attack vectors and threats discussed in Sections 3 and 4 above. At the very outset, a well-trained, and informed workforce is the first line of defense against malware. This includes periodic cybersecurity training and awareness programs, and appropriately designed tests and challenges to ascertain the level of preparedness of the organization. In the subsections below, we delve into specific defense mechanisms on several important domains. But before doing so, given the prevalence of Microsoft software and products in the marketplace we'd be remiss if we did not mention Microsoft's Security Compliance Toolkit[3]. The toolkit permits security professionals to test and apply security recommendations for most Microsoft products within their corporate network.

Firewall Hardening Using Open-Source Software

It is common knowledge that ransomware makes its way into an organization via file download, watering hole attacks, unsecured backdoors, email, malicious attachments, or via remote network protocols. To this end, it behooves the security professionals to harden firewall measures including, but not limited to (Sophos White Paper, 2021):

2 https://www.cisa.gov/stopransomware

3 https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

- Limiting or locking down remote desktop protocol, remote access, and management applications.
- Eliding all unwanted port forwarding and open ports in the firewall rules table.
- Support the latest TLS cipher suites and standards for ingress and egress traffic.
- Upgrading firewall equipment and related IT security devices to the current security standards.
- Ability to isolate traffic from infected systems.

Small and medium-sized businesses would be hard-pressed to find better solutions than the open-source offerings put forth by pfSense[4] and OPNsense5[5]. Both these providers have teamed up with hardware manufacturers to develop turn-key solutions for businesses of all sizes. Finally, we conclude this subsection on firewalls by pointing the reader to the special publication 800-41, by NIST SP 800-41 Rev. 1, "Guidelines on Firewalls and Firewall Policy" from the computer security resource center (Karen Scarfone, 2009). Despite being dated, this publication offers a detailed treatment of firewall technologies, architectures, and policies that will assist security administrators at SMBs as they deploy their network infrastructure.

Deploying Host and Network Intrusion Detection Systems

The increase in ransomware specifically targeted individuals in organizations and SMBs. Since such targeted attacks may bypass perimeter defenses such as firewalls, defense-in-depth strategies are necessary. Cyber threats, including ransomware, can be countered with intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). When used against known, less sophisticated attacks, such as those carried out by activist groups or large-scale email scams, they can be reasonably effective. These attacks are likely to be less effective against sophisticated, targeted attacks by criminals or state-sponsored hackers since they are more likely to use zero-day exploits and conceal their activities. This implies that they may also need to be part of a defense-in-depth strategy that involves encrypting sensitive information, maintaining detailed audit trails, implementing strong authentication and authorization controls, and actively managing the operating system and application security. The SMB should deploy a hybrid IDS which combines information from a number of sensors. Specifically:

a. In a host-based IDS (HIDS), suspicious activity is detected via examining the characteristics of a host and events occurring on that host, such as process identifiers and system calls. The primary advantage of a host-based IDS is that it can detect both external and internal intrusions, which is not possible either with network-based IDSs or firewalls.

b. In a network-based IDS (NIDS), monitoring and analysis are conducted on the network traffic and application protocols in order to detect suspicious activity.

A combination of Sagan[6], a free HIDS tool long with Snort[7], a free NIDS tool will be a powerful combination tool for IDS.

Best Practices for Business Recovery and Disaster Recovery Procedures

Risk mitigation and disaster recovery are components of most business continuity strategies to recover from a disaster, including ransomware. Lack of security controls and disaster recovery

4 https://www.pfsense.org/
5 https://opnsense.org/
6 https://quadrantsec.com/sagan_log_analysis_engine/
7 https://www.snort.org/

strategies may cause a financial impact on the business, which is almost impossible to recover. Generally, the complexity and development of such business continuity plans are handled by experts from a third party. However, having a consultant external to the organization can be an expense that is not justifiable for SMBs. The operating budget for this type of business is uncertain when it comes to protecting technology assets. More and more organizations, including SMBs, are migrating towards cloud computing due to its advantages and ease of maintenance. However, consumers and SMB users are worried about their loss of data on the cloud and data backup to their premises. No doubt, the cloud provides redundancy, but even this data is all, offsite. Consumers need to have their own data on-premises to eliminate dependency on CSP and need to secure this data. The proposed solution is a user deployment scenario by incorporating an application on a Linux box that will perform the backup of the cloud onto local drives. The application will interface with the cloud on a secured channel, check for updates and sync them with local storage. The data transmission will be secure and encrypted. This will provide a few advantages for the SMB.

1. Daily and monthly full backups can be done locally.
2. Since storage space in the cloud can be downsized because of local storage, the cost of the cloud can be reduced.
3. Migration from one cloud to another or from public to private or vice versa would be easier since the data is also available locally.

Limiting the Number of Services/Daemons on the SMB network

Recon is the first step of the Computer Network Attack (CNA) stage. During this stage, the attacker attempts to gather as much data as possible about the target in hopes of using it in subsequent stages of an attack, including Ransomware. Methods and tools used can vary from collecting data via Open-Source Intelligence (OSINT) tools such as search engine results, social media searches, and domain name registry data lookups, to social engineering attempts such as in-person or phishing attacks, and dumpster diving. Technical reconnaissance such as ping, Nmap, and Tracert can also be used. Some techniques, such as planting key loggers and sniffing the network for plain- text credentials, can take a varied amount of time before producing results. In addition to the ones listed above, resources available at centralops.net, osintinsight.com, and onstrat.com contain a multitude of online tools for OSINT data collection. Network reconnaissance, or the process of mapping the network using available tools, requires access to available information as well as the network. Generally speaking, the less information that is made available, the fewer the attackers are able to deduce. For starters, one can limit the information available in the domain registration records, which are public. Using generic role accounts eliminates names and protects against social engineering attacks. Prohibiting zone transfers on your DNS servers limits the amount of detail regarding your hostnames/IP addresses an attacker may receive. Moving on to actual active scanning, the general rule is to disable all unused services, ports, and protocols, as well as protecting any servers and applications that do not specifically need to be publicly accessed. Access to the network (physically and wireless) should be prohibited (such as 802.1X) unless specifically allowed. This will prevent the attacker from accessing the network. After these steps are taken, ongoing internal network reconnaissance should be performed in order to identify exactly what an attacker would see and make adjustments if necessary.

Scan is the next step and builds upon the port scanning and network mapping that may have been completed during the Recon phase. By looking for more detailed information regarding in-use applications and operating system specifics, the attacker may better identify vulnerabilities with which to focus their efforts on. This stage will include tools for network discovery and security auditing such as Wireshark, Nmap (also referenced in the prior stage), Nessus or OpenVAS,

Metasploit, Microsoft Baseline Security Analyzer, eEye's Retina, and GFI Languard. For example, the ability to assess web server and database versions may allow for the identification of known vulnerabilities, such as a SQL injection attack. Defending against scanning is approached most often by not allowing the scanner/attacker on the network, closing/disabling ports that will provide data to the scanner, or in some cases it is even possible to invalidate scanner results by moving services to a port other than what their services are generally accepted to be run on, such as moving ftp services off port 21, or moving another service to port 21. This can confuse the attacker and cause additional effort.

Antivirus and Related Software

Anti-virus software needs to be used on each end system. This gives the software maximum access to information on not only the behavior of the malware as it interacts with the targeted system but also the smallest overall view of ransomware activity. Fourth-generation antivirus programs, such as Malwarebytes and Windows Defender consist of a variety of anti-virus techniques, including scanning and activity trap components that are required. In addition, such a package includes access control capability, which limits the ability of ransomware to penetrate a system and then limits the ability of ransomware to update files in order to propagate.

PREVENTION TECHNIQUES

In this section, we outline some of the most prevalent approaches used in preventing some of these attacks.

Creation of a Security Policy and Appropriate Awareness Training

It is important to develop an organizational security policy that describes the objectives and strategies to thwart ransomware attacks and how they will be achieved. It is more common to have a set of related documents in an organizational or corporate security policy. This policy should cover:

1. The policy's intent and scope.
2. The interrelationship between the organization's businessgoals, legal and regulatoryduties, and security goals.
3. IT security needs for privacy, availability, accountability, authenticity, and dependability, especially in light of asset owners' perspectives.
4. The delegating of duties for the administration of IT security and the organizational infrastructure.
5. The organization's strategy for managing risk.
6. How to handle security awareness and training concerns with general employees, particularly for those in positions of trust.
7. Any potential legal consequences for staff members and the circumstances in which they would be applicable.
8. Security integration in system development and acquisition.
9. Contingency and business continuity planning.
10. Incident detection and handling processes.
11. How and when this policy should be reviewed.
12. The method for controlling changes to this policy.

The intent of the policy is to provide a clear overview of how an organization's IT infrastructure supports its overall business objectives in general, and more specifically what security requirements must be provided to do this most effectively.

Weakest link: The Human Factor - Social Engineering Attacks

Social engineering assaults are one of several avenues for launching ransomware-attacks, and as it turns out, also the most effective technique. The best line of defense against social engineering fraud in the SMB is awareness raised through the company cultures, training programs, and education. To become a "human firewall," a workforce must be taught how to identify and respond to an attacker's tactics. Simply following policy guidelines is not enough. The following actions should be included in a thorough countermeasure training program:

- Carry out a data classification evaluation to determine which workers have access to what categories and levels of private company data. Be aware of who a social engineering strategy is likely to use as its main target. Keep in mind that every employee faces a risk.
- Even if the individual claims to be a coworker, boss, or IT representative, never provide private or sensitive information to someone you don't know or who doesn't have a good reason to obtain it. If a password needs to be provided, it should never be communicated over email or phone.
- Refrain from conducting all financial transactions via email. Establish call-back policies with clients and vendors for all outgoing fund transfers to a pre-established phone number, if email must be used, or put in place a customer verification system with comparable dual verification capabilities.
- Create processes for independently verifying any modifications to vendor or customer information.
- Prevent utilizing or investigating "rogue devices" such as software on a computer or network or unauthenticated thumb/flash drives.
- Be wary of unsolicited emails and only open those that come from reliable sources. Never respond to or view links or attachments in such emails; instead, quarantine or delete them.
- Refrain from reacting to any offers received by phone or email. If something seems too good to be true, it most likely is. Unsolicited offers to help with a problem, such as a computer problem or other technical difficulty, could fall under this category.
- Be wary of anyone who tries to rush a conversation (act now, think later), refuses to offer basic contact information, uses threatening language, or demands confidential information. Before being disposed of in any on-site containers, such as dumpsters, physical documents and other tangible materials like computer hardware and software should always be shredded and/or destroyed.
- Actively address workplace information security complacency by putting in place internal awareness and training programs that are regularly reviewed with staff members. This entails creating an incident reporting and tracking program to keep track of social engineering incidents and putting an incident response plan into practice.
- Teach customer service representatives to spot the psychological tricks that social engineers employ, including pressure, speed, enticement, and power. If something is crucial enough to move on fast, it is crucial enough to confirm.

- Consider running a periodic, independent penetration test to evaluate the vulnerabilities in your company, such as unauthorized calls or emails to staff members asking for private information.
- Prevent unlawful physical access by adhering to rigorous rules for the display of security badges and other identification, and by ensuring that all visitors are escorted. Please turn away anyone who is "tailgating." Secure all important places, including executive offices, mail rooms, phone closets, and server rooms, always.
- To avoid sensitive information being exposed online, keep an eye on how social media platforms, public sources, and online commercial information are used.

Two-factor Authentication Techniques

The employment of multiple authentication methods in a system is referred to as multifactor authentication. The quantity of factors an authentication system incorporates heavily influences the system's strength. Systems that combine three elements are stronger than systems that just contain two of the components, and so on. Implementations that employ two factors are thought to be more effective than those that use just one factor.

While the primary authentication mechanisms are based on something that the individual knows, such as password and pin numbers, there are three other mechanisms that can be employed as part of the two-factor authentication techniques.

a) Something the individual possesses (token), such as electronic keycards, fobs, smart cards, and physical keys.

b) Something the individual is (static biometrics), such as getting recognition by fingerprint, retina, and face.

c) Something the individual does (dynamic biometric), such as getting recognized by voice pattern, handwriting characteristics, and typing rhythm.

When implemented and used correctly, each of these techniques can offer safe user authentication. Each approach, though, has drawbacks. A password could be susceptible to guessing or theft by an attacker. Similarly, an adversary may be able to steal or counterfeit a token. A user might misplace a token or forget their password. Additionally, maintaining and protecting the password and token information on systems entails a considerable administrative burden. There are many issues with biometric authenticators, such as handling false positives and false negatives, user acceptance, cost, and convenience. However, considering the cost factor and easy of access/use, the SMB should rely on face-recognition done by a mobile device (smartphone) of the user to provide authorization and authentication.

Principle of Least Privilege and Network Segmentation

The sorts of users on the system, their rights, the kinds of information they can access, and how and where they are defined and validated should all be taken into account during the system planning process. There will be users with enhanced privileges who can manage the system, typical users who can share appropriate access to files and other data as needed, and possibly even guest accounts with very restricted access. Restricting elevated rights to only those people who need them is a crucial mitigation technique for ransomware attacks. Furthermore, it is ideal for such individuals to only utilize systems with elevated rights when necessary to complete a task and to use them normally otherwise. By giving an attacker a limited window of opportunity to take advantage of the actions of such privileged users, increases the security profile of the system. In

order to help administrative users, elevate their privileges only when necessary and properly track these operations, certain operating systems offer specialized tools or access mechanisms.

Updating Operating systems and Software: Timely Security Patches

Securing the base operating system, which serves as the foundation for all other applications and services, is a crucial initial step in system security. An appropriately installed, patched, and configured operating system is necessary for a strong security foundation. Unfortunately, convenience and utility are frequently prioritized over security in many operating systems' default configurations. Additionally, as every firm has different security requirements, so will the proper security profile and, consequently, configuration.

It is essential that the system be kept as current as possible, with all crucial security-related patches implemented, given the ongoing discovery of software and other vulnerabilities for widely used operating systems and applications. This is undoubtedly one of the most important ransomware mitigation techniques. Today, almost every system that is frequently used comes with programs that can download and apply security updates automatically. To reduce the amount of time any system is exposed to vulnerabilities for which patches are available, these tools should be set up and used. It may be necessary to stage and validate all patches on test systems before deploying them in production for systems where availability and uptime are crucial. However, this procedure ought to be completed as soon as possible.

Lifecycle of a Ransomware Attack

In this section, we briefly outline the lifecycle of a ransomware attack as illustrated in Figure 1 below. As expected, once the malware has found a foothold using any of its attack vectors (phishing, trojan, or software vulnerability), it launches its attack. This is then followed by the infection phase, whereupon the malware contacts the command center to download the encryption key from the perpetrator. Once downloaded, this key is used to encrypt the victim's system which permits the next phase, the encrypt and extort phase. In this phase, a ransom message is made available on the victim's machine with directions on how the ransom is to be paid. Typically, this is done via Bitcoin or other unregulated mechanisms of cryptocurrency, for obvious reasons. Once the ransom is paid, the hope is that the victim is permitted to decrypt their data and proceed to the post-attack and data-recovery phase. It is of course in the interest of the attacker to propagate the virus and to this end, the virus continues to search for new victims and spread this cycle all over again.

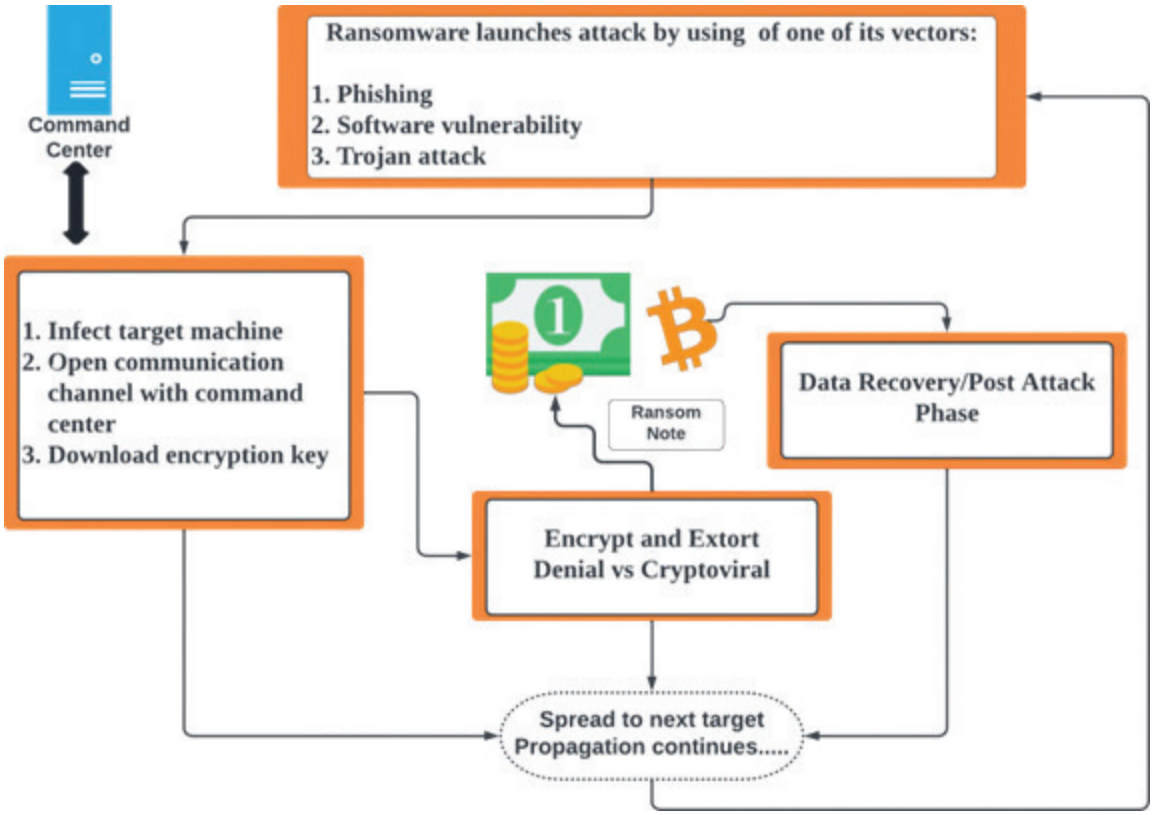

Figure1: Lifecyle of a ransomware attack

Planning a Response/Recovery After an Attack

We've spent quite a bit of time discussing various security measures to protect an SMB from ransomware attacks. Despite best efforts, attacks do indeed succeed and in this section, we briefly touch upon recovery techniques after an attack. Often, depending on the specifics of the attack, a victim does not have the luxury of time. To prevent further damage, the first response ought to be limiting the spread of the malware through the SMB network. To this end, isolation of infected hosts, disconnecting them from the network, disabling Wi-Fi, Bluetooth, and other communication channels is paramount. Having isolated the infected machines, identify the strain of malware that is plaguing these systems and report this to the authorities. In particular, victims are encouraged to file a complaint with the Internet Crime Complaint Center (IC3) by the FBI. Details on the procedure and what is to be included in the complaint are available here: https://www.ic3.gov/. Subsequently, use any of the above-mentioned strategies to restore affected systems and get the business running again.

The Future of Ransomware: Internet and the IoT

In this whitepaper, we asserted that an adaptive approach is necessary when dealing with ransomware as malware authors continually evade security software and deployed hardening measures. Ransomware is here to stay, and it can be forecasted to affect other systems and technologies like IoT. IoT, the Internet of things, encompasses all objects that are embedded with sensors, processing, and other tools that network them to other devices over the Internet or other large/small-scale networks. With the pervasiveness of the Internet and IoT, a far greater number of hosts are now in jeopardy from ransomware. For example, the connected-car can become a primary target as commands can be sent to essentially render the car inoperable until a ransom is paid. A similar

fate could await our mobile devices as well. In conclusion, ransomware defense tactics require a new approach that uses behavioral analysis and key traits common to ransomware to thwart their advance. To this end, the solutions we have put forth will therefore be applicable in many distinct applications and several different small and medium-sized business arenas to minimize downtime and lost profits/revenue to ransomware.

Conclusion

In conclusion, it is unfortunate that ransomware has now become an ever-present threat in our current marketplace. Several federal and state agencies have recognized this issue. In particular, ransomware is now classified as a federal crime and is reportable to the FBI as discussed in Section

8. The Federal Trade Commission, FTC, has a few publications "Cybersecurity for Small Business"[8] and "Ransomware prevention: An update for businesses"[9] aimed at helping small and medium-sized businesses. These publications have been created with input from NIST[10] (The National Institute of Standards and Technology), the SBA[11] (The U.S. Small Business Administration), and DHS[12] (United States Department of Homeland Security). We hope that this whitepaper and the resources mentioned herein help SMBs thwart any future ransomware attacks.

Acknowledgement

The authors would like to thank the Homeland Security Institute, and The Department of Computer Science at Sam Houston State University, for funding and support in developing this whitepaper.

References

Karen Scarfone, P. H. (2009). *Guidelines on Firewalls and Firewall Policy; Recommendations of the National Institute of Standards and Technology*. Information Technology Laboratory, Computer Security Resource Cente. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved July 27, 2022, from https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

Sophos White Paper. (2021). *Firewall best practices to block ransomware*. Sophos. Retrieved July 28, 2022, from https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/firewall-best-practices-to-block-ransomware.pdf

Suggested citation: Shashidhar, N., Varol, C. (2023). Ransomware Prevention and Defense: A hardening guide for small and medium-sized business. *One Step Ahead,* April 2023, 10-20.

8 https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
9 https://www.ftc.gov/business-guidance/blog/2020/12/ransomware-prevention-update-businesses
10 https://www.nist.gov/
11 https://www.sba.gov/
12 https://www.dhs.gov/

DETECTING DRONE (UNMANNED OR UNCREWED AERIAL SYSTEM) THREATS AT STADIUMS (STADIA) AND PUBLIC VENUES: FRAMING THE ISSUE

Nathan P. Jones
John P. Sullivan
George W. Davis

This technical paper will frame the issue of current and protentional threats to homeland security posed by Unmanned Aerial Systems (UAS), commonly and hereby referred to as drones, on public stadiums.[1] In the immediate post 911 environment, the US government weaponized drones for the targeting of terrorists.[2] This had numerous advantages including not risking US personnel (both pilot and support personnel near combat zones) and minimizing the physical infrastructure in place around the world needed for manned operations. The Predator and Reaper drones were effective in targeting terrorists both in terms of pattern of life surveillance, but also as a platform for hellfire missiles, and assassination.[3] Little thought was given to the fact that as this technology became more ubiquitous and cheaper, other states, terrorists, and criminals would eventually use this technology against US national and homeland security interests.

This technical paper will discuss these, and other threats posed to US critical infrastructure through the lens of drone threats to public stadiums and large gatherings, with an illustrative discussion of drone traffic over the Astroworld concert/festival. While drones were not used maliciously at Astroworld, mapping and analyzing the drone activity at this crowded and lethal public event, supplies a window into the complexity of drone detection, counter drone measures, and the challenges future security personnel will need to overcome to defend US critical infrastructure in an era of cheap ubiquitous drones.

Drones are not novel. Animals such as mules, have long been used as unmanned drones for smuggling operations, reducing the risk of arrest for human smugglers here on the Texas border dating to the 19th century and earlier.[4] Hobbyists have used remote controlled airplanes and helicopters for decades. What has changed in the 21st century is the cost of drones, their capabilities resulting from rapid advances in various technologies, and enhanced capabilities derived from free US government public utilities such as the global positioning system (GPS). These new technologies include software and internet-based interconnection of software development, the global positioning system (GPS), networked communication improvements, battery technologies, and the lower cost of electronic hardware such as semiconductors, computer processors, and other components. The reduced costs and weights of these technologies have made drones ubiquitous, and the future promises drone saturation with the Government Accountability Office (GAO) predicting more than 2 million drones by 2024 comprised of 800,000 commercial and more than 70% recreational.[5] This situation will and has called for increased regulation and government capacities to address it, a topic addressed here later and in the third technical paper of this series.[6]

Drones and Sporting/Mass Public Events

The United Nations has identified drone attacks on public stadiums and critical infrastructures as an emerging threat.[7] Scholars such as Robert J. Bunker have also identified the threat of terrorist and insurgent drones to mass events and the potential for mass casualties.[8] Scholars have identified the potential for terrorists to use drones to disperse chemical or biological weapons.[9] While these attacks may have a low probability of success, as so many biological and chemical attacks led by terrorists have failed, a potential attack may cause mass panic in a crowded stadium leading to crowd control issues and mass casualty events.

According to Federal Aviation Administration (FAA) regulations, drones are prohibited at public stadiums with more than 30,000 people. This includes one hour before and after scheduled play time for Major League Baseball (MLB), National Football League (NFL), National Association for Stock Car Auto Racing (NASCAR), and National Collegiate Athletic Association (NCAA) Division 1 Football. The FAA has developed public service announcements working with the stadium managers association (SMA) to remind people not to use drones in and around games.[10]

There are many examples of drones disrupting public stadiums and sports events, e.g., the 2017 crash landing of a drone in PETCO Park in San Diego, which nearly injured several fans.[11] Stadium security personnel and local law enforcement are limited in what they can do to counter drones. First, they cannot shoot drones down legally and even if they could that would pose public safety risks. Stadiums cannot hijack the drone through software and force it to land or jam its signal. Thus, they are typically forced to find the pilot and deter or mitigate the threat by dispatching security or law enforcement to the pilot.[12] Many individuals are unaware they have broken laws related to drones, but others do so intentionally at multiple public stadiums. The company, Airsight had already blacklisted one drone pilot at one stadium after an illegal flight which allowed the company to send an immediate alert to the stadium when the individual showed up at Wrigley Field.[13]

In a case study report on the Camping World Stadium in Orlando Florida, Airsight summarized their drone detections on the days of the Camping World Bowl Game, the Citrus Bowl, and the NFL Pro Bowl. In one incident, during the Pro Bowl, 2 unauthorized drones were detected across 3 flights and Orlando Police were alerted to the pilot location based on detection data provided.[14] Geofencing of a restricted area via geographic software mapping make these alerts possible. Sports stadiums are not the only areas where mass gatherings occur, and drones can be a potential threat. Areas such as the Las Vegas strip have also seen potentially dangerous drone activity. In one incident the FAA contacted a private drone detection company to identify a particularly dangerous flight. This is an example of the close cooperation between public and private entities necessary to critical infrastructure protection.[15]

Astroworld: The Travis Scott Concert

This three-part technical series of papers will discuss and analyze drone threats to public stadiums through the lens of the Astroworld event. The Astroworld Festival concert headlined by Travis Scott in Houston on 5 November 2021 resulted in 10 deaths as concert goers suffered injuries in the crowd against the stage as Travis Scott performed. There were also significant injuries earlier in the day as concert goers rushed barricades resulting in crowd related injuries.[16] Emergency personnel treated dozens for injuries at the concert and in local hospitals.[17] During the concert the Houston Police Department declared a mass casualty event in conjunction with the Houston Fire Department. While Scott claimed not to know the crowd injured concert goers, according to ABC News he stopped his set three times to point out injured individuals, but continued his set.[18] Previous Travis Scott Concerts had posed public safety issues and Scott had been accused of inciting violence at concerts in which “raging” was encouraged.[19] Scott had pleaded guilty to dis-

orderly conducted charges resulting from inciting concert goers to jump barricades in 2015 and 2017.[20] The 2021 concert resulted in at least 30 lawsuits against Travis Scott and Live Nation, the company in charge of the event. The image below provides a visual representation of the area of the concert in red within the Houston geographic context. It is a 3D model of the relevant area generated by the authors.

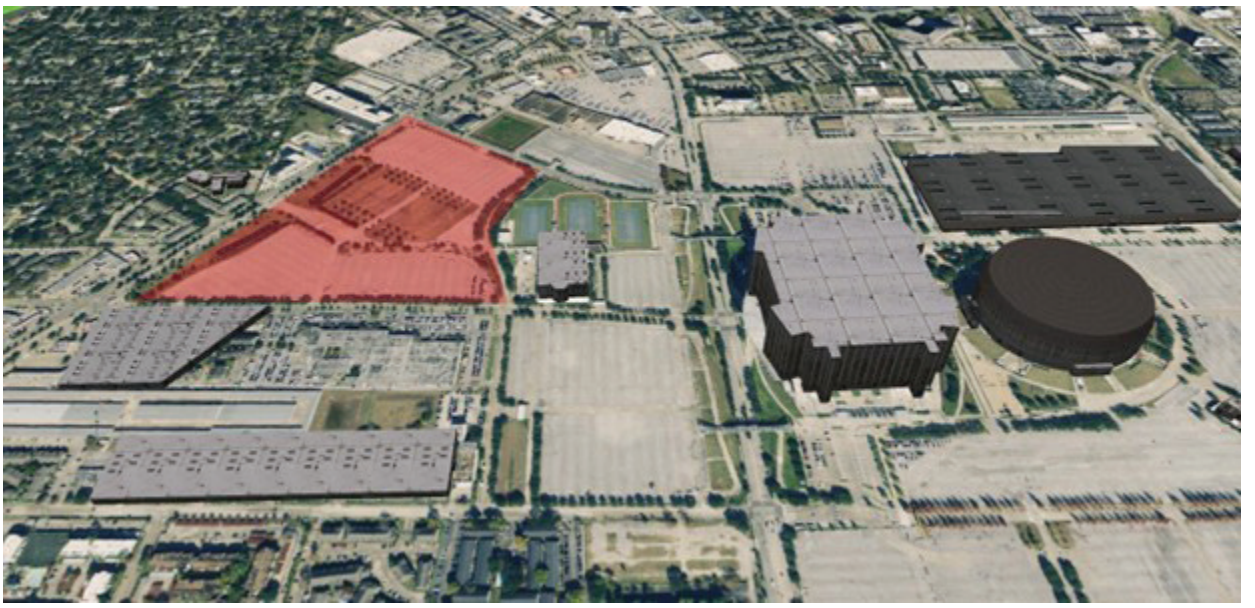

Figure 1. 3D Model of Astroworld Event and Environs (Festival Event Depicted in in Red).

The events of Astroworld Houston 2021 also precipitated a state of Texas commissioned taskforce producing a report to set up policies to prevent future concert mass casualty events.[21] The concert resulted in the detection of abnormally large drone traffic which points to possible threats to public security at public stadiums. Significant drone activity at an event like Astroworld could result in collisions between drones and emergency vehicles such as helicopters, harm crowds on the ground, or could be an attack site for terrorists or other malevolent actors.

Figure 2. A depiction of an intruder drone in close proximity to a rescue helicopter in a 3D Scene (Authors' elaboration).

The potential for drone traffic to damage or hinder emergency operators during mass casualty events are the types of situations emergency managers and incident commanders will need to prepare for as drones increase in ubiquity.

Exploratory Analysis of the Airsight Data Related to Astroworld

As part of this project on drone threats to public stadia, the Dallas based drone detection company Airsight provided the researchers with drone detection data derived from sites near the Astroworld event. The drone detection methods and layers will be discussed in-depth in technical paper 3 of this series, but a preliminary sense of the data is useful. The data included the dates of 4-7 November 2021, so that the researchers could assess patterns in the data prior to, during, and after the Astroworld Concert tragedy of 5 November 2021. The data set was narrowed to a half mile square radius around the Astroworld concert. Within these parameters, 12,666 data points were collected, though it should noted that a majority of these were the same drone, or drone flight, being detected at multiple points along its flight path. Despite this high number of data points only 25 unique drone IDs were present, while only 46 unique flight IDs were present in the period. This is consistent with Airsight analysis of their own data on other sporting events.[22] Figure 3 below breaks the data down by drone type, which are primarily Da- Jiang Innovations (DJI) drones, a ubiquitous Chinese manufactured brand.

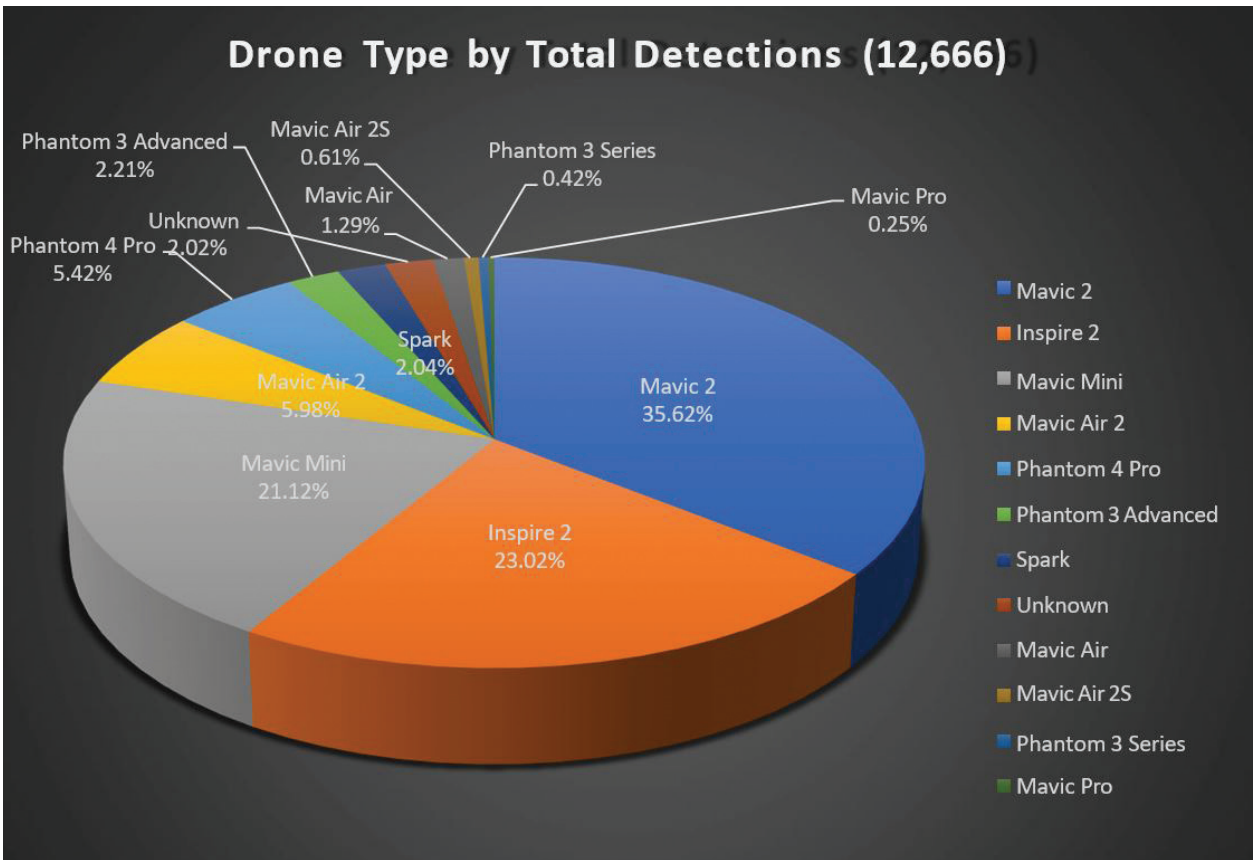

Figure 3. Drone Detections by Drone Type (Authors' Analysis)

Drone type trends can serve to alert incident commanders to the potential payload capacities and therefore threat types present in the operational environment. The Appendix to this technical paper contains numerous tables and charts summarizing the data. One table summarizes the altitude data for all flights, every time the drone was detected. We see the maximum altitude was 499.5

feet while the minimum detected was 3 feet below sea level suggesting there may have been topographically low points near the site or detection error issues. The average height of the drones across all flight detections was 36.87 feet across the full set of 12,666 detection over 46 flights.

One key finding was that drone activity increased during the event (evening of 5 November) and surged the day after the event on 6 November. Local news reported on crowds rushing the gates and injuries posted to local websites at 3:15pm on the day of the concert 5 November may have led to increased drone activity.[23] It is plausible that drone operators may have launched drones to survey the area based on these reports.

Much like closed circuit television (CCTV) footage, many drone detection systems monitor critical infrastructure, but detect other relevant data from surrounding events, allowing investigators to piece data together after the fact. This requires significant analytical capability to analyze disparate systems. In the near future artificial intelligence systems may play a key role in piecing these varying data streams together immediately after events and in real time. As the subsequent papers in this project will demonstrate, the Astroworld event on 5 November 2021, is a useful cases study in drone traffic. The primary uptick in drone traffic was the day after the event, suggesting media, hobbyists, personal injury lawyers, and law enforcement may have been particularly interested in surveilling and documenting the event in its aftermath. For a video analysis of drones over Astroworld during and after the event see the Institute for Homeland Security at Sam Houston website.

Conceptualizing Potential Homeland Security Drone Threat Actors: The Illicit, the Unwitting, and the Foreign Power

Here it may be useful to divide the discussion on potential drone threats into three categories, the illicit, the unwitting, and the foreign power or foreign power proxy. In the first category are malign actors such as terrorists, criminals, or corporate espionage actors, with violent or illicit profit-motive in mind. In the second category, the unwitting, are the unintentionally malign. These might include individuals wishing to have video footage of a major sports stadium event and be unaware of laws and regulations, or individuals flying drones unwittingly in restricted areas. While homeland security may tend to focus on the first category, the second category, the unwitting, through sheer numbers, is today the bigger problem for critical infrastructure, leading to jammed flight paths, damage from accidents, disruption from response security measures, etc. Drones in and around airports or the flight paths of manned emergency flight vehicles is also a threat to US critical infrastructure. The third category, foreign power or foreign power proxy, category includes state actors such as foreign governments engaging hybrid warfare and great power competition.[24] These activities may include, use of airspace, espionage, sabotage activities, information warfare dissemination, cyberthreats, etc. Foreign powers also seek plausible deniability and thus may use proxies such as organized crime actors to carry out their operations against the United States and its interests.[25]

Illicit non-state actors have already used drones to damage US homeland Security. These activities include Mexican organized crime groups (OCGs) using drones for surveillance of US law enforcement agency activities and movements to smuggle drugs in the United States.[26] Terror networks also use drones. These include terrorist bombings be they conventional, dirty bomb, chemical or bioweapon attack, or pre/post attack intelligence, surveillance, and reconnaissance (ISR). Terrorists have used drones to even the playing field in terms of costs. For example, in 2017, in Syria ISIS used a drone to drop a landmine inside a stadium. The resulting fire caused damage far more than the cost of the attack.[27] Corporate, nation state, or illicit network actors can use drones for espionage.

Illicit networks can use drones as loitering munitions as they have already been used in conventional battles.[28] The 2020 war between Azerbaijan and Armenia in which Azerbaijan decisively defeated the Armenians using Israeli designed loitering munitions made armies around the world take note of loitering munitions.[29] Loitering drone munitions are an emerging technology which have received significant social media and news attention due to the role they play in the 2022 Russian invasion of Ukraine. The announcement the US government military aid package to Ukraine in mid 22 would include the switchblade "kamikaze" drone system garnered significant attention. Brian Devereaux argues that loitering munitions systems should be treated separately from drones, because they are a "smart" or "loitering missile" as one manufacturer AeroVironment calls them.[30] These systems can loiter "30-60 minutes, while some Israeli systems can loiter for nine hours."[31] Once airborne they cannot be recovered and will likely be expended quickly.

Similarly, drones can be used for aerial networking on the battlefield by both benevolent and malicious actors.[32] While this is most likely to be nation-state actors, the pattern is that what is the purview of the state rapidly succumbs to "the democratization of technology" be it for good or ill.[33] Drones can be used to disrupt flight paths for critical infrastructure such as airports or harass defenders of other critical infrastructures such as public stadia.[34] Drones can deliver contraband into prisons or play other roles in nefarious prison activity such as facilitating escapes. Nefarious actors can use drones to fly over physical infrastructure and become potential WIFI spoof cyber threats.[35]

Soon we can expect new drone-based threats including multiple simultaneous drone terror attacks[36] used in conjunction with other attack types such as those employed in Mumbai 2008.[37] While this "swarming" and "lethal autonomous weapon systems" (LAWS) technology will initially be developed by nation-states, non-state actors will inevitably replicate it.[38]

Counter-Drone Measures (C-UAS)

We can conceptualize drone counter measures/counter-unmanned aerial systems (C-UAS) along a continuum of impact upon the drone, the pilot, and society. At the low end of the spectrum are

1) physical barriers such as netting to prevent drone entry and or the dropping of contraband by drones into prisons. Drones can be 2) jammed via radio signals forcing them to land in place or return via pre-programed routes. Drones can be 3) blinded via directed energy weapons such as lasers if they are relying on optical sensors for piloting. 4) Drones can be spoofed to take control of and capture the drone. Drones can be 5) destroyed via directed energy weapons or projectiles. Drones are much like planes and can be shot from the sky in the same fashion via anti-aircraft fire.[39] This however is less viable outside wars zones and around civilian infrastructure. Firing projectiles in the air comes with the risk of where the munition will ultimately fall to the ground.

6) The drone pilot can be targeted, (questioned, warned, detained, arrested, incapacitated, or in the case of violent ongoing crime: killed (extreme)) before, during, or after an event which has, is, or will impact critical infrastructure security. All of the previously mentioned countermeasures may one day also be delivered by drones themselves, which may have the effect of allowing these processes to be more precisely delivered with minimal threat to innocents and automated through artificial intelligence systems.

The Regulatory Environment

As previously mentioned, the FAA has instituted numerous regulations related to drones including piloting license requirements, which are not onerous and not in person, requiring new drones to broadcast information about them and the pilot, and regulations banning drones in certain areas such as during major sporting events. As of 2022 only four federal government agencies

(Department of Defense (DOD), Department of Justice (DOJ), Department of Homeland Security (DHS), and the Department of Energy (DOE)) are legally able to use certain counter drone measures in limited circumstances, which may include signal jamming wherein the drone is either pre-programmed to land or return home. There are other countermeasures depending upon the size and altitude of the drone. In the future we may see more directed energy weapons (lasers, microwave, etc.) used as counter drone measures. These types of measures may have the advantage of rapidly responding to drone swarms, which can overwhelm defenses. One of the key hindrances to practical counter drone measures, is the limited number of agencies and personnel with counter drone authorization. Most public stadia events will be under the purview of local and state actors, which under the current regulatory scheme must depend on the four federal agencies with these capabilities. Conversely, there are good reasons to limit the expansion of counter drone measures. Jamming technologies could disrupt commercial flights potentially disrupting passenger planes, or Life Flight public health infrastructure helicopter communications.

The second paper in this series discusses operational perspectives on responding to drone threats at public stadia while the third paper addresses the technical aspects of developing situational awareness and a common operational picture to counter potential drone threats. The third paper also concludes the series with policy recommendations.

Appendix

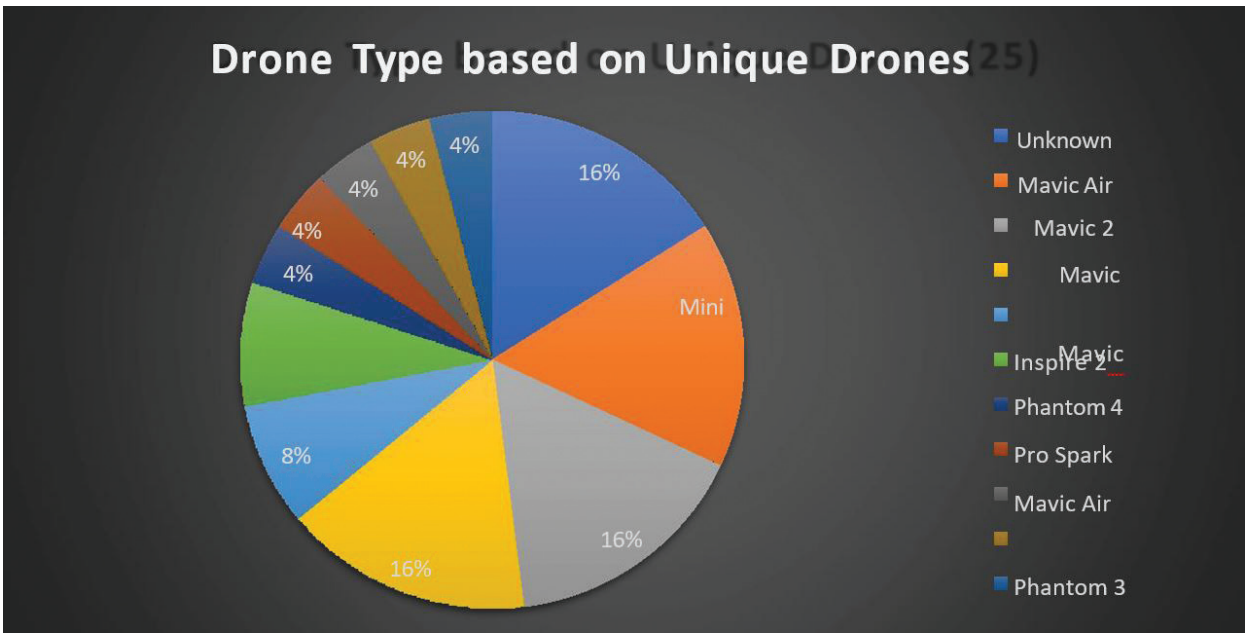

Figure 4. Drone Detections by Unique Drone (Authors' Analysis)

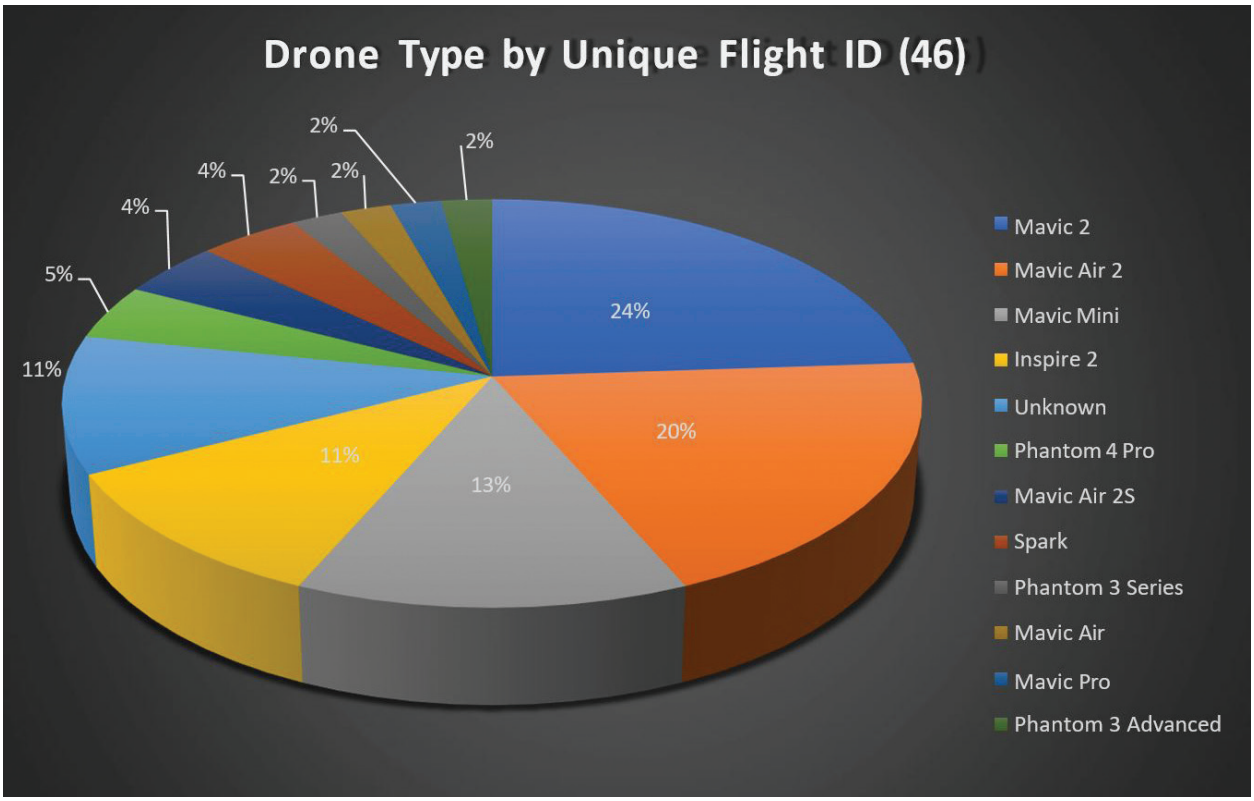

Figure 5. Drone Type by Unique Flight ID (Authors' Analysis)

Table 1: Analysis of Detected Drone Altitude

Altitude in Feet	
Mean	36.8746408
Standard Error	0.52477079
Median	20.8
Mode	0
Standard Deviation	59.0594491
Sample Variance	3488.01853
Kurtosis	14.0155548
Skewness	3.24514193
Range	499.5
Minimum	-3.7
Maximum	495.8
Sum	467054.2
Count	12666
Confidence Level (95.0%)	1.02863014

Table 2: Analysis of Detected Drone Speed

Speed	
Mean	0.99851571
Standard Error	0.02161973
Median	0
Mode	0
Standard Deviation	2.43315583
Sample Variance	5.9202473
Kurtosis	9.28448619
Skewness	3.09539026
Range	14
Minimum	0
Maximum	14
Sum	12647.2
Count	12666
Confidence Level (95.0%)	0.04237793

Author Bios

Nathan P. Jones is an Associate Professor of Security Studies in the college of Criminal Justice at Sam Houston State University. He is the author of Georgetown University Press's peer reviewed book Mexico's Illicit Drug Networks and the State Reaction (2016). His areas of interest include organized crime violence in Mexico, drug trafficking organizations, social network analysis, border security, and the political economy of homeland security. Dr. Jones is also a Senior Fellow with the Small Wars Journal - El Centro, a Rice University Baker Institute Drug Policy and US-Mexico Center non-resident scholar, and the Book Review Editor for the Journal of Strategic Security. Prior to joining the Sam Houston State University Security Studies Department, Dr. Jones was the Alfred C. Glassell III Postdoctoral Fellow in Drug Policy at Rice University's Baker Institute for public policy, where his research focused on drug violence in Mexico.

Dr. John P. Sullivan was a career police officer, now retired. Throughout his career he has specialized in emergency operations, terrorism, and intelligence. He is an Instructor in the Safe Communities Institute (SCI) at the University of Southern California, Senior El Centro Fellow at Small Wars Journal, and Contributing Editor at Homeland Security Today. He served as a lieutenant with the Los Angeles Sheriff's Department, where he has served as a watch commander, operations lieutenant, headquarters operations lieutenant, service area lieutenant, tactical planning lieutenant, and in command and staff roles for several major national special security events and disasters. Sullivan received a lifetime achievement award from the National Fusion Center Association in November 2018 for his contributions to the national network of intelligence fusion centers. He has a PhD from the Open University of Catalonia, an MA in urban affairs and policy analysis from the New School for Social Research, and a BA in Government from the College of William & Mary.

George W. Davis Jr. specializes in providing technology solutions to the defense and public safety sectors. He is a specialist in geospatial Information Systems and Geospatial Intelligence (GEOINT). After the 9/11 2001 attacks at the World Trade Center he supported the Emergency Mapping and Data Center (EMDC), mapping the area around Ground Zero as well as most of Manhattan

south of Canal Street. He served as Geospatial Information Coordinator for the New York Metro Chapter of Infragard. He has worked with the Department of Homeland Security (DHS), New York Police Department (NYPD), FBI, Los Angeles Sheriff's Department (LASD), the Lower Manhattan Security Initiative, and the Business Emergency Operations Center (BEOC) Alliance in New Jersey. Projects included mapping and aerial photography for several national and international disasters (Hurricanes: Charley, Katrina, Rita, Ike and Hugo), the Haiti Earthquake and the Sri Lanka Tsunami, using LIDAR, 3D Modeling software, Unmanned Aerial Systems (Drones), Thermal Imaging, Ground Penetrating Radar (GPR), GPS, and other remote sensing technologies.

Endnotes

1 Another term often used in the literature is Unmanned Aerial Vehicle (UAV). Declan Walsh, "Foreign Drones Tip the Balance in Ethiopia's Civil War," New York Times, 20 December 2021, https://www.nytimes.com/2021/12/20/world/africa/drones-ethiopia-war-turkey-emirates.html.

2 Brian Bennett, "Predator Drones Have yet to Prove Their Worth on Border," Los Angeles Times, 28 April 2012, http://articles.latimes.com/2012/apr/28/nation/la-na-drone-bust-20120429; Daniel R. Brunstetter, "Can We Wage a Just Drone War?," The Atlantic, 19 July 2012, https://www.theatlantic.com/technology/archive/2012/07/can-we- wage-a-just-drone-war/260055/.

3 Aki Peritz and Eric Rosenbach, Find, Fix, Finish: Inside the Counterterrorism Campaigns That Killed Bin Laden and Devastated Al Qaeda, Paperback (New York: Public Affairs, 2013).

4 George T. Díaz, Border Contraband: A History of Smuggling Across the Rio Grande (Austin: University of Texas Press, 2015).

5 "Science, Technology Assessment, and Analytics: Counter-Drone Technologies," Spotlight (Washington, D.C.: Government Accountability Office, March 2022), https://www.gao.gov/assets/gao-22-105705.pdf; Bart Elias, "Protecting Against Rogue Drones," In Focus (Washington, D.C.: Congressional Research Service, 14 May 2020), 1.

6 J. "Matt" Rowland and Chris Fleischer, "Why State and Local Law Enforcement Needs Legal Authority from Congress to Counteract Dangerous Drones," Police1, 10 October 2021, https://www.police1.com/police- products/police-drones/articles/why-state-and-local-law-enforcement-needs-legal-authority-from-congress-to- counteract-dangerous-drones-Cer6e9HCGbfZvDRr/.

7 The report goes on to describe drone attacks by terrorists which often target civilians as reaching their targets 70% of the time. "Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies" (United Nations, 2021), 29–30, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/211006_guide_on_security_major_sp orting_events_web.pdf.

8 Robert J. Bunker, "Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications" (Carlisle, PA: US Army War College, Strategic Studies Institute, 2015).

9 Bunker, 18; Suzanne Sincavage and Candice Carter, "17. Unique Challenges of Responding to Bioterrorism & Chemical Threats & Attacks Delivered by Drones," in Drone Delivery of CBNRECy – Dew Weapons Emerging Threats of Mini-Weapons of Mass Destruction and Disruption (WMDD), ed. Randall Nichols et al., 2022, https://newprairiepress.org/ebooks/46.

10 "Drones Are Prohibited In and Around Stadiums," Federal Aviation Administration, 27 May 2022, https://www.faa.gov/uas/resources/community_engagement/no_drone_zone/stadiums.

11 Emma Baccellieri, "As Drones Take Off, MLB Has to Play Defense," Sports Illustrated, 11 February 2021, https://www.si.com/mlb/2021/02/11/drone-footage-baseball-stadiums-security.

12 Baccellieri.

13 911 Security referenced in the article rebranded to Airsight during this research. See Baccellieri.

14 "UAS: Flight Data: Orlando Florida & Camping World Stadium," Case Study (Dallas: Airsight, September 2020), https://www.911security.com/hubfs/PDF%20Downloads/911%20Security%20Orlando%20UAS%20Case%20Study%20-%20Sept%202020%20v1.2.pdf.

15 "Case Study: Las Vegas - Drone Detection in Action," Airsight, 2019, https://www.911security.com/blog/case- study-las-vegas-drone-detection-in-action.

16 "Report from the Texas Task Force on Concert Safety," (Austin, TX: Texas Taskforce on Concert Safety Report, 19 April 2022), https://gov.texas.gov/uploads/files/press/2022_Report_Texas_Task_Force_on_Concert_Safety.pdf. 17 "Astroworld Festival Timeline: How the Tragedy Unfolded," ABC News, 18

November 2021, https://abcnews.go.com/Entertainment/astroworld-festival-timeline-tragedy-unfolded/story?id=81036039.

18 "Astroworld Festival Timeline."

19 Joe Coscarelli, "Before the Astroworld Tragedy, Travis Scott's 'Raging' Made Him a Star," New York Times, 8 November 2021, https://www.nytimes.com/2021/11/08/arts/music/travis-scott-astroworld-concerts.html.

20 "Astroworld Festival Timeline."

21 "Report from the Texas Task Force on Concert Safety," (Austin, TX: Texas Taskforce on Concert Safety Report, 19 April 2022), https://gov.texas.gov/uploads/files/press/2022_Report_Texas_Task_Force_on_Concert_Safety.pdf.

22 "UAS: Flight Data: Orlando Florida & Camping World Stadium."

23 "Crowds Storm through Astroworld Gates," KPRC, 5 November 2021, https://www.click2houston.com/video/local-news/2021/11/05/crowds-storm-through-astroworld-gates-/.

24 Chad Briggs, "Climate Change and Hybrid Warfare Strategies," Journal of Strategic Security 13, no. 4 (December 2020): 45–57, https://doi.org/10.5038/1944-0472.13.4.1864.

25 On plausible deniability and covert operations see Mark M. Lowenthal, Intelligence: From Secrets to Policy, 8th ed. (Thousand Oaks: Sage: CQ Press, 2019).

26 Organized crime has used drones for smuggling across the US-Mexico border, thus enhancing the profits and corruptive influence of OCGs. A destabilized Mexico has obvious homeland security implications for US border security and potentially overwhelming drug, weapon, and refugee/immigration flows. Robert J. Bunker and John P. Sullivan, Criminal Drone Evolution: Cartel Weaponization of Aerial IEDs (Bloomington: XLibris, 2021).

27 Mansji Asthana, "Watch: How A $500 Drone Annihilates A $500 Million Stadium In Syria," The Eurasian Times, 28 October 2020, https://eurasiantimes.com/watch-how-a-500-drone-annihilates-a-500-million-stadium-in- syria/.

28 Delharty Manson, "Swarmed States: The Impact of Small Loitering Munitions on Weak Regimes" (Williamsburg: Project on International Peace and Security, 2022), https://www.wm.edu/offices/global-research/research- labs/pips/white_papers/2021-2022-white-papers/delharty-manson-whitepaper.

29 Brennan Deveraux, "Loitering Munitions in Ukraine and Beyond," War on the Rocks, 22 April 2022, https://warontherocks.com/2022/04/loitering-munitions-in-ukraine-and-beyond/.

30 Deveraux.

31 Deveraux.

32 Colin Demarast, "US Army Reaches for the Sky to Solve Communication Needs," Defense News, 21 June 2022, https://sports.yahoo.com/us-army-reaches-sky-solve-114051387.html.

33 Thomas L. Friedman, The Lexus and the Olive Tree: Understanding Globalization (Farrar, Straus and Giroux, 2000).

34 "Department of Defense Counter-Unmanned Aircraft Systems" (Washington, D.C.: Congressional Research Service, 31 May 2022), https://sgp.fas.org/crs/weapons/IF11426.pdf.

35 Edwards and Harold, "June 2022."

36 Zachary Kallenborn, Gary Ackerman, and Philipp C. Bleek, "A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism," Terrorism and Political Violence (20 May 2022): 1–30, https://doi.org/10.1080/09546553.2022.2061960.

37 Don Rassler and Muhammad al-'Ubaydi, "Anticipating Future Directions of Tech-Enabled Terror," Lawfare, 12 December 2021, https://www.lawfareblog.com/anticipating-future-directions-tech-enabled-terror.

38 John R. Hoehn, Kelley M. Sayler, and Michael E. DeVine, "Unmanned Aircraft Systems: Roles, Missions, and Future Concepts" (Washington, D.C.: Congressional Research Service, 18 July 2022), 17–18, https://www.everycrsreport.com/files/2022-07-18_R47188_93558486445fb635720ded1a6526f33c0a4f5602.pdf.

39 Drones can also be targeted by trained birds such as eagles. Dutch police tested this possibility but found the birds difficult to train.

Suggested citation: Jones, N.P., Sullivan, J.P., Davis, G.W. (2023). Detecting Drone (Unmanned of Uncrewed Aerial System) Threats at Stadiums (STADIA) and Public Venues: Framing the issue. *One Step Ahead,* April 2023, 21-31.

TEXAS CRITICAL INFRASTRUCTURE HEALTHCARE SUPPLY CHAIN PROTECTION

Scott Lynn

INTRODUCTION

The Homeland Security Institute of Sam Houston State University commissioned this paper as part of a series of papers regarding marketing the need for Supply Chain Preparation, Response, Resilience and Recovery to the four Texas Critical Industries (Health Care, Energy, Chemical and Transportation).

Supply chain disruptions will occur – it is not a question of "if" but "when." They may come from natural disasters, industrial accidents, internal or external attackers, but they will come. Preparing for them is the best way to help Texas Critical Infrastructure stay online, in business and prepared to serve the people of the state. Providing recommendations on how to gain the ear of the businesses making up the Texas health care industry is what this paper will attempt to provide. This specific paper discusses:

1. What Health Care sectors are most important to protect in the event of a supply chain disruption, and approximately how many health care businesses of various sizes exist in Texas.
2. Healthcare supply chain requirements, especially for Trauma and Long-Term Care facilities.
3. Potential supply chain threats affecting health care (focused around critical infrastructure).
4. Healthcare community responses to Supply Chain Disruptions
5. Existing resources available to the Health Care industry for supply chain protection.

Note that this document does not include facility susceptibility electronic vulnerability. While that is an extremely critical concern, it is beyond the scope of this document.

HEALTHCARE SECTORS DESIGNATED AS "CRITICAL INDUSTRIES"

This section defines what Texas businesses can be classified approximates as Healthcare Critical Industry businesses. It also provides an approximation of their numbers and sizes.

Most "critical and vulnerable" healthcare sectors

For the purposes of this paper, not all healthcare sectors were considered "most" critical and

vulnerable. Selected health care areas were because:

1. They are essential in saving lives in an emergency.
    a. This includes trauma centers and regular hospitals.
2. Losing them would cause loss of life, whether in an acute or long-term condition.

   a. The “long-term” description is intended to add in rehabilitation centers, convalescent hospitals, long-term care and assisted living facilities.

3. Their loss would affect other necessary infrastructure.
   a. With respect to healthcare, this is primarily envision conditions where the inability to treat would result in large numbers of people not being able to perform their own work (examples: Covid-driven isolation and its effect on the supply chain, blood banks, or healthcare staff availability).

4. Their loss would have a psychological effect on the people of the state leading to panic, hoarding or other undesirable events.
   a. “Psychological effects” are multi-faceted. They can range from hoarding (an example being toilet paper in the early days of Covid), to the effect on patients not having access to psychiatric care or medications.

Functionally, this paper defines Healthcare “Critical Industries” as hospitals, walk-in surgical centers, medical laboratories, ambulance services, Long Term Care (LTC) facilities, and assisted living facilities.

Defining Critical and Non-Critical Sectors - NAICS Codes

This paper uses North American Industry Classification System (NAICS) codes to approximate the number of businesses of each type in Texas. NAICS codes are a standardized method used to define business types. As they are used by the US Census bureau in gathering data, they also allow approximation of the number of businesses of each category for each US state and county.

Table 1 below uses US Census 2017 Annual Business Survey data to estimate the number of businesses of each type which fall under Healthcare CI, and should benefit for SCD planning.

Note that the part of Table 1 containing “621xxx” NAICS codes does not include all business types that exist under that category. They are listing as “Non-CI Businesses” in Table 2.

Healthcare NAICS Codes Considered as Critical “Industries”

The following table shows the number of businesses of each NAICS category, and what portion of that category is a “small” (less than 100 employees) or a “large” (more than 100 employees) business.

Table 1: Texas CI Businesses and sizes

Outpatient or Home Health Care							
NAICS Code	NAICS Description	<100 Employees			100+ Employees		
621420	Outpatient Mental Health and Substance Abuse Centers	349	(73%)		129	(27%)	
621492	Kidney Dialysis Centers	51	(7%)		731	(93%)	
621493	Freestanding Ambulatory Surgical and Emergency Centers	497	(56%)		396	(44%)	
621498	All Other Outpatient Care Centers	587	(58%)		428	(42%)	
621511	Medical Laboratories	345	(39%)		538	(61%)	
621512	Diagnostic Imaging Centers	447	(67%)		221	(33%)	
621610	Home Health Care Services	2,797	(70%)		1,210	(30%)	
621910	Ambulance Services	291	(54%)		249	(46%)	
621991	Blood and Organ Banks	15	(9%)		160	(91%)	
621999	All Other Miscellaneous Ambulatory Health Care Services	341	(80%)		86	(20%)	
	Sub-Totals:	5,720	(58%)		4,148	(42%)	
Hospitals and Related Services							
NAICS Code	NAICS Description	<100 Employees			100+ Employees		
622110	General Medical and Surgical Hospitals	45	(10%)		398	(90%)	
622210	Psychiatric and Substance Abuse Hospitals	4	(6%)		62	(94%)	
622310	Specialty (except Psychiatric and Substance Abuse) Hospitals	10	(8%)		110	(92%)	
	Sub-Totals:	59	(9%)		570	(91%)	
Long-term care and assisted living							
NAICS Code	NAICS Description	<100 Employees			100+ Employees		
623110	Nursing Care Facilities (Skilled Nursing Facilities)	572	(36%)		1,000	(64%)	
623210	Residential Intellectual and Developmental Disability Facilities	216	(15%)		1,243	(85%)	
623220	Residential Mental Health and Substance Abuse Facilities	180	(66%)		93	(34%)	
623311	Continuing Care Retirement Communities	200	(61%)		127	(39%)	
623312	Assisted Living Facilities for the Elderly	499	(53%)		442	(47%)	
623990	Other Residential Care Facilities	135	(61%)		85	(39%)	
	Sub-Totals:	1,802	(38%)		2,990	(62%)	

The significance of this is that it shows the number of smaller businesses in each sector and the percentage of those in each sector which is small vs. large. This will be discussed further in the section on factors affecting supply chain disruptions.

Healthcare NAICS Codes Not Considered as "Critical Industries"
This paper focuses on larger institutions caring for multiple patients within one facility and especially offering life-support functions. Therefore, the business below are omitted from the "Critical Industry" list.

Table 2: Non-CI Businesses and sizes

Non - CI Businesses by NAICS and number of employees						
Outpatient or Home Health Care						
NAICS Code	NAICS Description	<100 Employees			100+ Employees	
621111	Offices of Physicians (except Mental Health Specialists)	17,330	(81%)		3,979	(19%)
621112	Offices of Physicians, Mental Health Specialists	870	(99%)		5	(1%)
621210	Offices of Dentists	10,706	(91%)		1,010	(9%)
621310	Offices of Chiropractors	2,409	(100%)		0	(0%)
621320	Offices of Optometrists	2,030	(99%)		28	(1%)
621330	Offices of Mental Health Practitioners (except Physicians)	1,552	(97%)		42	(3%)
621340	Audiologists	1,855	(70%)		777	(30%)
621391	Offices of Podiatrists	421	(100%)		0	(0%)
621399	Offices of All Other Miscellaneous Health Practitioners	1,570	(91%)		147	(9%)
621410	Family Planning Centers	145	(76%)		46	(24%)
		38,888	(87%)		6034	(13%)

HEALTHCARE SUPPLY CHAIN REQUIREMENTS AND VULNERABILITIES

Healthcare Supply Chain Items
Abbreviations used below are:

Item Type	Abbreviation	General Use	Abbreviation
Patient Care	Pt.C.	Consumable	Cons.
Equipment	Equip.	Management Too	MT

Below is a list of various items used in hospitals and related healthcare facilities, their use and general type, as well as what upstream Texas Critical industries affect their availability. Someone needing items listed on the left would be well advised to be aware of events in the four CIs listed to the right.

Table 3: CI Supply Chain Needs

Required Item In The Supply Chain	Use	Item Type	Texas Critical Industry Affecting Supply Chains			
			Health care	Energy	Chemical	Transpor-tation
Blood	Pt. Care	Cons.	x	x		x
Food loss / spoilage	Pt. Care	Cons.		x		x
Medications / pharmaceuticals	Pt. Care	Cons.		x	x	x
Medical supplies (consumables and devices for patient treatment	Pt. Care	Cons.		x	x	x
X-Rays and CT Scanning equipment	Process	Equip.		x		
Medical gases	Pt. Care	Cons.		x	x	x
Immunizations	Pt. Care	Safety	x	x	x	
Inventory distribution	Process	-		x	x	x
Cleaning	Process	Cons.		x	x	
Disinfectants	Process	Cons.			x	x
Oxygen (piped and tanks)	Pt. Care	Cons.		x	x	x
Distributed Refrigeration in (departments)	Process	Equip.		x		
Durable medical devices	Pt. Care	Equip.		x	x	
MRO	Process	Equip.		x	x	x
Electricity loss	Pt. Care	Utility		x	x	
Fuel (heating, sterilization, cleaning)	Process	Utility		x	x	x
Vacuum	Process	Utility		x		
Compressed Air	Process	Utility		x		
Water	Process	Utility		x		
Wastewater	Process	Utility		x		
Water filtration	Process	Utility		x	x	
Inventory Control	MT	-		x		x

Medical Supply Chain Vulnerabilities

Below is a partial list of the above supply chain vulnerabilities, their possible origin points, and possible cascading effects downstream of the disruption point.

Supply Chain Vulnerabilities

- Consumable product availability
- Consumable device availability
- Physical Supply Chain (PSC) attack
- Central supply (inventory management & ordering) disruption
- Medical devices (Durable medical equipment) operation
- Electric power (longer than 24 hours required by Texas law)
- Heat loss (boilers, space heat)
- Water quality
- Wastewater system disruption
- Food Supply
- Overloading / pandemic effect on supply chain (excess demand).
- Data communication (internal and external)
- Record security / corruption
- Data input and extraction

Sources of Supply chain attacks

- External infrastructure attack (power or inventory)
- Employee sabotage
- Vendor supply chain or manufacturing disruptions - Consumables
- Inbound Transportation disruption
- Weather
- Vendor supply chain or manufacturing disruptions - MRO
- Pandemic

Inbound cascading effects

- Treatment capability (pharmaceutical & device function)
- Treatment capability (inventory)
- Sterilization & cleaning (water and fuel)
- Pharmaceuticals availability
- Pharmaceuticals quality
- Medical device availability
- Medical device quality
- Patient health & nutrition

Outbound cascading effects

- Contagion / Pandemic
- Health / Death
- Inability to turn around patients

FACTORS AFFECTING SUPPLY CHAIN DISRUPTIONS

Hospitals, ambulatory care, and Long-Term/Assisted Living facilities operate under different regulations, have different sizes, levels of complexity, regulations under which they operate, urban vs. rural locations, etc. A discussion of these factors follows.

Business Size and Resources

Per US Census data, the number of small and large Texas healthcare businesses is as follows:

Per 2017 US Census data:

- 90% of hospitals have more than 100 employees
- 38% of nursing and residential care facilities have fewer than 100 employees.
- 58% of Outpatient or Home Health Care facilities have fewer than 100 employees.

Effectively, this means that Outpatient or Home Health and Long-Term care / Assisted Living facilities tend to be smaller, with fewer resources for emergency planning than larger facilities.

The effect of size on shutdowns caused by supply chain disruptions is complex. Disruptions are more likely to affect small businesses than larger ones, but the effect on the area is greater when a large business shuts down. Therefore both have valid arguments as they compete for scarce resources in an emergency.

Likewise, smaller businesses are less likely to be specifically targeted for a disruption, but transportation to remote areas may make them more vulnerable to supply chain disruptions.

Last, small businesses often have less money available for significant expenditures which might bolster emergency preparedness.

Complexity of Service
Healthcare facilities must deal with complexities unmatched by most businesses. In addition to basic utilities, patients will have different needs, resulting in plethora of different types of care and medicines. Therefore, medical inventories therefore must be highly varied - what a Disney supply chain executive referred to as “mass boutique”.

Healthcare vulnerabilities will primarily be based on the type of service organizations provide. *In general, the more complex and / or comprehensive the services provided, the higher the vulnerability.*

Location
Simply put, the closer a facility is to a distribution point, the more likely it is to be able to receive supplies.

CRITICAL INDUSTRY SUPPLY CHAIN DISCUSSION

Energy
As shown in the Supply Chain Needs table above, electricity is required to supply or operate every aspect of healthcare. It runs life support equipment, refrigeration, lighting, record keeping, vacuum systems and other equipment, making it the most critical of the Critical Infrastructures.

Different types of healthcare facilities in Texas have different backup requirements for backup generator operating time, as follows:

> **Hospitals** without natural gas fuel to have maintain on-site fuel storage for 48 hours for emergency backup generators serving equipment which, if it fails, will cause death or patient harm.1[1]
>
> **Ambulatory (Walk-In Surgery) Care Centers** are required to have eight hours fuel for backup power for areas serving surgery.2[2]

1 Texas Administrative Code Title 25, Part 1, Chapter 131, Subchapter G, Rule §131.141
2 Title 25, Part 1, Chapter 135, Subchapter C, Rule §135.52

Skilled Nursing Facilities with Category 1 and Category 2 equipment, must have four hours of fuel located on-site.3[3]

Long-term / Assisted Living Facilities are not required to have backup power beyond that required for emergency lighting and exit signs.4[4]

Federal Medicare / Medicaid regulations do require LTCs to have an emergency plan for what to do in the event of a power failure. The regulations do require the facility to Include strategies for addressing emergency events identified by the risk assessment."5,6[56]

Energy supply chain disruptions

In addition to loss of facility power, Texas health care facilities have experienced the following during outages:

- Power losses shutting down HVAC systems, resulting in patient discomfort and, in at least one case, death from a loss of power during a severe cold spells.7[7]
- When outages lasted longer than the legislated fuel reserve times, Long Term / Assisted Living Facilities have had to purchase additional fuel.
- Fuel supplies for which LT/AL facilities have contracted have been diverted to other users.
- Generators have not been available or had to be transported in from remote locations.
- Diesel fuel has become too viscous to flow, resulting in a generator failure.
- Because Propane-driven generators emit carbon monoxide, people have died due to improper generator operation or venting.

Chemical

The chemical supply chain is also critical in hospital supply chains. A failure in the chemical supply chain may not immediately affect hospital operations but, SCD effects can, depending on the chemical, be felt quite quickly.

Petrochemicals

Petrochemical uses include:

- Natural Gas For Heating Fuels
- Propane For Backup Generators

Pharmaceutical Manufacturing

Pharmaceutical manufacturing is heavily dependent on chemical availability, whether used as ingredients, catalysts, or for packaging. A disruption here would affect the manufacturing of pharmaceuticals.

3 Title 26, Part 1, Chapter 554, Subchapter D, Division 9, Rule §554.361
4 Title 26, Part 1, Chapter 553, Subchapter D, Divisions 4-11, Electrical Requirements
5 https://files.asprtracie.hhs.gov/documents/aspr-tracie-cms-ep-rule-long-term-care.pdf
6 Code of Federal Regulations (81 CFR 63859)Medicare and Medicaid Programs; Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers
7 https://www.kxan.com/investigations/which-texas-senior-living-facilities-have-backup-power-state-waiting-on-survey-results/#:~:text=All%20skilled%20nursing%20facilities%20and,48%20hours'%20worth%20of%20fuel.

Plastics Manufacturing
All plastics are chemically derived. Their use is ubiquitous in health care. The following list shows some uses of plastic-derived products:

- Medical Devices
- Syringes
- Silicone Tubing
- Medical Supply Containers
- Packaging for blood, plasma, saline and other liquids
- Catheters

Petrochemical Loss Effects
Petrochemical losses have affected:

- Backup power generator operating time
- HVAC systems (Heating)
- Boilers (space heating, water heating, washing and sterilization)
- Availability of consumable devices (medical devices and packaging)

The loss of raw materials for consumable supplies does not manifest itself as quickly as other SCDs but, if it affects availability of medical devices, this quickly becomes a major problem. New chemical formulations or even switching to non-FDA-approved suppliers requires an approval process that can take months or years. This in turn makes a “simple” raw material disruption extremely important.

At least one Texas RAC reported plastics shortages affecting the supply of bags used for tasks such as blood, plasma, or other liquid deliveries.

Medical Gases
Medical Gases include Medical Air, oxygen, carbon dioxide, nitrogen, nitrous oxide, helium and others. While some are generated on site, many facilities use bottled gasses.

When electricity is disrupted, the ability of gas generators to operate is disrupted. Whether on-site of offsite, a loss of power means they are unable to operate. It is worth noting that many gas generators are relatively local to their customers. Widespread power outages can affect both the supplier and the customer, affecting the delivery of oxygen, nitrogen, CO2 and other gases used for medical procedures.

Transportation
To date, the major way SCD disruptions have been manifested in Texas is by extreme storms (hurricanes or freezing) causing flooding or shutting down operations. Some examples of these follow.

Trucks deliver virtually every item consumed in health care facilities except electricity and natural gas. While hospitals try to maintain three days of supplies on hand, a loss of in-

bound food and supplies will quickly disrupt operations. Weather, labor strikes or anything disrupting their operation will rapidly become visible.

Just-in-time ordering has magnified the importance of transportation. While many hospitals formerly had warehouses, reducing operating costs moved them to reduce or eliminate them. Health care facilities now order largely on a just-in-time basis, and typically stock only three days of supplies.

Effect on patients
The effect of transportation SCDs is most felt with frail or fragile patients. During storms, sheltering in place is safer than moving frail them, and is the first option used by healthcare facilities. This makes maintaining transportation or preparing for its disruption critical for life safety.

Effects on hospitals
Trauma facilities which failed in the last floods were the larger, not the smaller ones.

Hurricanes and power outages also result in “Patient Flooding.” During emergencies, RACs and local healthcare agencies have experienced both people coming to hospitals to shelter and emergency responders dropping groups of rescued patients at the hospitals. These “unexpected guests” require additional supplies in order for the hospital to care for them.

Effects on pharmaceutical delivery
During storms, pharmaceutical compounders or re-packagers supplying Long Term Care facilities have shut down. As a result, LTC facilities have had to work with non-contracted suppliers who were not ready for volume orders. They in turn needed to order and deliver pharmaceuticals, subjecting them to SCDs.

Effects on isolated populations
These, due to being smaller or isolated from main logistics streams, are especially subject to transportation SCDs.

1. Their orders are typically smaller, resulting in lower priority.
2. They may not be as aware of alternative suppliers as are larger companies with well-developed and redundant supply chains.
3. Pharmaceutical suppliers not contracted to or supplied by large companies have not been prepared for emergency volume orders
4. Smaller (especially privately owned) care facilities don’t always have the resources to plan for SCDs have experienced shortages. Cameron Tilton of the Texas Assisted Living Association was quoted as saying “about half the assisted living communities in Texas serve 16 or fewer residents”. Many of them are “private pay,” meaning they don’t receive the same kind of Medicaid reimbursements as skilled nursing facilities.”8[8]
5. Their physical remoteness makes them more susceptible to road or airport closures.

8 8 https://theworldlive.news/Which-Texas-senior-living-facilities-have-backup-power-State-waiting-on-survey- results-504125

6. In areas with high undocumented alien populations, suspicion of state or federal authorities leads them to not "connect" to available supply chain resources. This was evidenced during the Covid pandemic.

HEALTHCARE COMMUNITY RESPONSES TO SUPPLY CHAIN DISRUPTIONS

The healthcare industry, especially the more established agencies, have developed a number of strategies to deal with Supply Chain Disruptions. A number of these follow:

Energy

- Local agencies will communicate with local facilities to encourage them to order fuel and backup generators. Likewise, they will work to turn local community centers into shelters.

Chemical

- When chemical supply chain disruptions affecting pharmaceuticals occur, RACs have lobbied the FDA to expedite new drug or device approval.
- Hospitals have worked to ensure alternate suppliers are available.
- The chemical supply chain (as it affects manufacturing of products used by hospitals) is an issue because hospitals cannot control it. Therefore, their option is to purchase larger quantities for storage or to go to alternate suppliers.

Transportation

- When storms are anticipated, TALA will try to work with pharmaceutical compounders and re- packagers to get advanced supplies.
- The Regional Advisory Commissions and groups like TALA will work with pharmaceutical compounders and re-packagers to get advanced supplies. If one supplier runs short, this gives them an alternative source.
- Under some conditions, the national stockpile may be accessed.

Other

1. Due to past experiences, the hospitals and related agencies exhibit a high degree of cooperation during disasters.
2. Both the Regional Advisory Councils and groups like TALA work to educate hospitals, LTACs, rehabilitation facilities and other healthcare organizations in their area.
3. Hospitals prepare for SCDs by discharging as many patients as possible.
4. RACs work with medical shelters, Long Term Acute Care (LTAC) facilities and rehabilitation facilities to provide shelter for the "unexpected guests".
5. TALA members have sister communities they will move residents to. Some own central pods containing supplies they will move to sites where they send residents.
6. Assisted Living associations will work with facilities to ensure they receive information about available disaster resources.
7. TALA will work with government agencies to turn community centers into shelters.

8. The RACs may also have Special Populations coordinators who can reach out to both hospitals and Long-Term Care facilities to offer assistance.

Gaps Or Needs Expressed
The biggest needs expressed have to do with maintaining power, supply stocks and hospital access. Following are a few ways RACs and TALA have recommended these goals are met.

- Government stockpiles are to be distributed to states within 12 hours of receiving requests. It has been requested that they distributed on a more local level if possible.
- Facilities sheltering patients, they should have enough food, water and supplies for a minimum of seven days (Joint Commission hospital certification regulations only require 96 hours).
- RAC and TALA clients need to improve their logistics awareness to minimize SCD effects.
- Partner with Red Cross to provide shelters, deliver water, MREs, etc.
- Ultimately, the legally required emergency preparedness plans need to be maintained. While they have been greatly improved, ensuring they are maintained and taken seriously by facilities is critical.

Last is the issue of getting the attention of healthcare providers. As a rule, people trust those with whom they are closest. This militates toward ensuring RACs, TALA and others are prepared to rapidly disseminate information to their clientele.

Appendix 1

Healthcare Emergency Planning Communication Channels

Texas Emergency Preparedness Organizations
Regional Advisory Committees

Texas has 22 geographically oriented Regional Advisory Councils (RACs) serving trauma care centers, nursing homes, long-term care and other healthcare facilities in their areas. Each RAC is required to develop, implementing, and monitoring a regional emergency medical service trauma system plan9,10[910].

The RAC headquarters is:

Texas Department of State Health Services 1100 West 49th Street
Austin, Texas 78756-3199
Phone: 512-776-7111
https://www.dshs.texas.gov/emstraumasystems/etrarac.shtm

Regional RAC web site addresses are as follows: TSAMap-RACNames.pdf

Northeast Texas RAC	https://www.netrac.org/
Piney Woods RAC	https://rac-g.org/
Deep East Texas RAC	http://www.detrac.org/
Far West TX & Southern New Mexico RAC	http://borderrac.org/
Texas “J” RAC	https://www.texasjrac.org/

9 9https://www.dshs.texas.gov/emstraumasystems/etrarac.shtm#:~:text=Regional%20Advisory%20Councils%20(RACs)%20are,medical%20service%20trauma%20system%20plan.

10 10 https://www.dshs.texas.gov/emstraumasystems/RegionalAdvisoryCouncils_History_Overview06_2008.pdf

Concho Valley RAC	http://www.cvrac.org/
Central Texas RAC	http://www.centraltexasrac.org/
Heart of Texas RAC	http://www.hotrac.org/
Brazos Valley RAC	http://bvrac.com/
Capital Area Trauma RAC	http://catrac.org/
Southwest Texas RAC	https://www.strac.org/
SouthEast Texas Trauma RAC	https://www.setrac.org/
East Texas Gulf Coast RAC	https://rac-r.com/
Golden Crescent RAC	http://www.gcrac.org/
Seven Flags RAC	https://sevenflagsrac.org/
Coastal Bend RAC	https://www.cbrac.org/
Rio Grande Valley Trauma RAC	https://www.tracv.org/

Texas Assisted Living Association

TALA is a trade association working with assisted living facilities. They also coordinate with HHS and RACs.

TALA sends out a monthly emails to members and non-members. They also hold monthly webinars, again both for members and non-members.

Texas Department of State Health Services

Texas Department of State Health Services
1100 West 49th Street
Austin, Texas 78756-3199
https://www.texasready.gov/

Texas Division of Emergency Management

1033 La Posada
Suite 300
Austin, Texas 78752-3824
(512) 424-2208
https://www.tdem.texas.gov/

Texas Health and Human Services, Division of Long-Term Care

1100 West 49th St. Austin, Texas 78756-3199
P.O. Box 149347
Austin, Texas 78714-9347
https://acl.gov/ltc

Federal / Other Emergency Preparedness Information Sources

Ready.Gov	https://www.ready.gov/
HHS.Gov	Hospital Preparedness Program https://aspr.hhs.gov/HealthCareReadiness/HPP/Pages/default.aspx
CMS.Gov	Centers for Medicare and Medicaid Services https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule
FEMA	FEMA.Gov; Emergency Management Institute Training https://training.fema.gov/nims/

FEMA Training Center For Domestic Preparedness (FEMA training)
https://cdp.dhs.gov/

CDC Supply Chain Disaster Preparedness Manual
https://www.cdc.gov/cpr/readiness/healthcare/supplychaindisasterpreparedness-manual.htm

NFPA Standard 1600, Standard on Continuity, Emergency, and Crisis Management
https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and- standards/detail?code=1600

Joint Commission Hospital and Hospital Clinics Manual
https://www.jointcommission.org/resources/patient-safety-topics/emergency-management/

Appendix 2

NAICS Codes Used

The following market segment definitions are taken from the US Census Bureau 2022 NAICS Reference Manual11[11]. It is intended to provide a more complete description of the businesses in each segment and what populations they serve.

621420 Outpatient Mental Health and Substance Abuse Centers

This industry comprises establishments with medical staff primarily engaged in providing outpatient services related to the diagnosis and treatment of mental health disorders and alcohol and other substance abuse. These establishments generally treat patients who do not require inpatient treatment. They may provide a counseling staff and information regarding a wide range of mental health and substance abuse issues and/or refer patients to more extensive treatment programs, if necessary.

Illustrative Examples

- Outpatient alcoholism treatment centers and
- clinics (except hospitals)
- Outpatient mental health centers and clinics (except hospitals)
- Outpatient detoxification centers and clinics (except hospitals)
- Outpatient substance abuse treatment centers and clinics (except hospitals)
- Outpatient drug addiction treatment centers and clinics (except hospitals)

Cross-References

- Establishments known and licensed as hospitals primarily engaged in the inpatient treatment of mental health and substance abuse illnesses with an emphasis on medical treatment and monitoring are classified in Industry 622210, Psychiatric and Substance Abuse Hospitals;
- Establishments primarily engaged in the inpatient treatment of mental health and substance abuse illnesses with an emphasis on residential care and counseling rather than medical treatment are classified in Industry 623220, Residential Mental Health and Substance Abuse Facilities;

11 https://www.census.gov/naics/reference_files_tools/2022_NAICS_Manual.pdf

- Establishments of physicians primarily engaged in the independent practice of psychiatry or psychoanalysis are classified in U.S. Industry 621112, Offices of Physicians, Mental Health Specialists;
- Establishments of independent mental health practitioners (except physicians) are classified in Industry 621330, Offices of Mental Health Practitioners (except Physicians); and
- Establishments primarily engaged in providing nonresidential counseling services for substance abuse, mental health, suicide intervention, and other crisis intervention social services to children and youth, the elderly, persons with disabilities, and all other individuals and families are classified in Industry Group 6241, Individual and Family Services.

62149 Other Outpatient Care Centers

This industry comprises establishments with medical staff primarily engaged in providing general or specialized outpatient care (except family planning center s and outpatient mental health and substance abuse centers). Centers or clinics of health practitioners with different degrees from more than one industry practicing within the same establishment (e.g., Doctor of Medicine and Doctor of Dental Medicine) are included in this industry.

Specific Subcategories selected as high urgency include:

621492 Kidney Dialysis Centers

This U.S. industry comprises establishments with medical staff primarily engaged in providing outpatient kidney or renal dialysis services.

621493 Freestanding Ambulatory Surgical and Emergency Centers

This U.S. industry comprises establishments with physicians and other medical staff primarily engaged in (1) providing surgical services (e.g., orthoscopic and cataract surgery) on an outpatient basis or (2) providing emergency care services (e.g., setting broken bones, treating lacerations, or tending to patients suffering injuries as a result of accidents, trauma, or medical conditions necessitating immediate medical care) on an outpatient basis.

Outpatient surgical establishments have specialized facilities, such as operating and recovery rooms, and specialized equipment, such as anesthetic or X-ray equipment.

Illustrative Examples
- Freestanding ambulatory surgical centers and clinics
- Freestanding emergency medical centers and clinics
- Freestanding trauma centers (except hospitals)
- Urgent medical care centers and clinics (except hospitals)

Cross-References
- Outpatient community health clinics with health practitioners from multiple industries are classified in U.S. Industry 621498, All Other Outpatient Care Centers; and
- Establishments known and licensed as hospitals that also perform ambulatory surgery and emergency room services are classified in Subsector 622, Hospitals.

621498 All Other Outpatient Care Centers

This U.S. industry comprises establishments with medical staff primarily engaged in providing general or specialized outpatient care (except family planning centers, outpatient mental health and substance abuse centers, HMO medical centers, kidney dialysis centers, and freestanding ambulatory surgical and emergency centers). Centers or clinics of health practitioners with different degrees from more than one industry practicing within the same establishment (e.g., Doctor of Medicine and Doctor of Dental Medicine) are included in this industry.

Illustrative Examples

- Outpatient biofeedback centers and clinics
- Outpatient pain therapy centers and clinics
- Outpatient community health centers and clinics
- Outpatient sleep disorder centers and clinics

62151 Medical and Diagnostic Laboratories

This industry comprises establishments known as medical and diagnostic laboratories primarily engaged in providing analytic or diagnostic services, including body fluid analysis and diagnostic imaging, generally to the medical profession or to the patient on referral from a health practitioner.

Illustrative Examples

- Dental or medical X-ray laboratories
- Medical pathology laboratories
- Diagnostic imaging centers
- Medical testing laboratories
- Medical forensic laboratories

Cross-References

- Establishments, such as dental, optical, and orthopedic laboratories, primarily engaged in providing the following activities to the medical profession, respectively: making dentures, artificial teeth, and orthodontic appliances to prescription; grinding lenses to prescription; and making orthopedic or prosthetic appliances to prescription are classified in Industry 33911, Medical Equipment and Supplies Manufacturing; and
- Establishments primarily engaged in providing health screening or physical fitness evaluation services (except by offices of health practitioners) are classified in Industry 62199, All Other Ambulatory Health Care Services.

621511 Medical Laboratories

This U.S. industry comprises establishments known as medical laboratories primarily engaged in providing analytic or diagnostic services, including body fluid analysis, generally to the medical profession or to the patient on referral from a health practitioner.

Illustrative Examples

- Blood analysis
- laboratories
- Medical pathology laboratories
- Medical bacteriological laboratories
- Medical testing laboratories
- Medical forensic laboratories

Cross-References

- Establishments known as dental laboratories primarily engaged in making dentures, artificial teeth, and orthodontic appliances to prescription are classified in U.S. Industry 339116, Dental Laboratories.
- Establishments known as optical laboratories primarily engaged in grinding lenses to prescription are classified in U.S. Industry 339115, Ophthalmic Goods Manufacturing;
- Establishments known as orthopedic laboratories primarily engaged in making orthopedic or prosthetic appliances to prescription are classified in U.S. Industry 339113, Surgical Appliance and Supplies Manufacturing; and
- Establishments primarily engaged in providing health screening or physical fitness evaluation services (except by offices of health practitioners) are classified in U.S. Industry 621999, All Other Miscellaneous Ambulatory Health Care Services.

621512 Diagnostic Imaging Centers

This U.S. industry comprises establishments known as diagnostic imaging centers primarily engaged in producing images of the patient generally on referral from a health practitioner. Illustrative Examples

- Computer tomography (CT-scan) centers
- Medical radiological laboratories
- Dental or medical X-ray laboratories
- Ultrasound imaging centers
- Magnetic resonance imaging (MRI) centers

621610 Home Health Care Services

This industry comprises establishments primarily engaged in providing skilled nursing services in the home, along with a range of the following: personal care services; homemaker and companion services; physical therapy; medical social services; medications; medical equipment and supplies; counseling; 24-hour home care; occupation and vocational therapy; dietary and nutritional services; speech therapy; audiology; and high-tech care, such as intravenous therapy.

Illustrative Examples

- Home health care agencies
- Visiting nurse associations
- Home infusion therapy services
- In-home hospice care services

Cross-References

- In-home health services provided by establishments of health practitioners and others primarily engaged in the independent practice of their profession are classified in Industry 62111, Offices of Physicians; Industry 621210, Offices of Dentists; Industry Group 6213, Offices of Other Health Practitioners; and U.S. Industry 621999, All Other Miscellaneous Ambulatory Health Care Services;
- Establishments primarily engaged in providing non-medical home care or homemaker services for the elderly or persons with disabilities are classified in Industry 624120, Services for the Elderly and Persons with Disabilities;
- Establishments primarily engaged in renting or leasing products for home health care are classified in U.S. Industry 532283, Home Health Equipment Rental; and
- Establishments primarily engaged in retailing home health care equipment are classified in U.S. Industry 456199, All Other Health and Personal Care Retailers.

6219 Other Ambulatory Health Care Services

This industry group comprises establishments primarily engaged in providing ambulatory health care services (except offices of physicians, dentists, and other health practitioners; outpatient care centers; medical laboratories and diagnostic imaging centers; and home health care providers).

621910 Ambulance Services

This industry comprises establishments primarily engaged in providing transportation of patients by ground or air, along with medical care. These services are often provided during a medical emergency but are not restricted to emergencies. The vehicles are equipped with lifesaving equipment operated by medically trained personnel.

Cross-References

- Establishments primarily engaged in providing transportation of the disabled or elderly (without medical care) are classified in U.S. Industry 485991, Special Needs Transportation.

621991 Blood and Organ Banks

This U.S. industry comprises establishments primarily engaged in collecting, storing, and distributing blood and blood products and storing and distributing body organs.

Cross-References

- Establishments primarily engaged in providing courier and express delivery services for blood, blood products, and body organs without storage are classified in Industry 492110, Couriers and Express Delivery Services.

621999 All Other Ambulatory Health Care Services

This industry comprises establishments primarily engaged in providing ambulatory health care services (except offices of physicians, dentists, and other health practitioners; outpatient care centers; medical and diagnostic laboratories; home health care providers; and ambulances).

Illustrative Examples

- Blood donor stations
- Pacemaker monitoring services
- Blood or body organ banks
- Physical fitness evaluation services (except by offices of health practitioners)
- Health screening services (except by offices of health practitioners)
- Smoking cessation programs
- Hearing testing services (except by offices of audiologists)

Cross-References

- Establishments primarily engaged in the independent practice of medicine are classified in Industry 62111, Offices of Physicians;
- Establishments primarily engaged in the independent practice of dentistry are classified in Industry 62121, Offices of Dentists;
- Establishments primarily engaged in the independent practice of health care (except offices of physicians and dentists) are classified in Industry Group 6213, Offices of Other Health Practitioners;

- Establishments primarily engaged in providing general or specialized outpatient care services are classified in Industry Group 6214, Outpatient Care Centers;
- Establishments primarily engaged in providing home health care services are classified in Industry 62161, Home Health Care Services;
- Establishments primarily engaged in transportation of patients by ground or air along with medical care, are classified in Industry 62191, Ambulance Services;
- Establishments known as medical and diagnostic laboratories primarily engaged in providing analytic or diagnostic services are classified in Industry 62151, Medical and Diagnostic Laboratories; and
- Establishments primarily engaged in providing courier and express delivery services for blood, blood products, and body organs without storage are classified in Industry 49211, Couriers and Express Delivery Services.

622 Hospitals

Industries in the Hospitals subsector provide medical, diagnostic, and treatment services that include physician, nursing, and other health services to inpatients and the specialized accommodation services required by inpatients. Hospitals may also provide outpatient services as a secondary activity. Establishments in the Hospitals subsector provide inpatient health services, many of which can only be provided using the specialized facilities and equipment that form a significant and integral part of the production process.

6221 General Medical and Surgical Hospitals 622110 General Medical and Surgical Hospitals

This industry comprises establishments known and licensed as general medical and surgical hospitals primarily engaged in providing diagnostic and medical treatment (both surgical and nonsurgical) to inpatients with any of a wide variety of medical conditions. These establishments maintain inpatient beds and provide patients with food services that meet their nutritional requirements. These hospitals have an organized staff of physicians and other medical staff to provide patient care services. These establishments usually provide other services, such as outpatient services, anatomical pathology services, diagnostic X-ray services, clinical laboratory services, operating room services for a variety of procedures, and pharmacy services.

6222 Psychiatric and Substance Abuse Hospitals 622210 Psychiatric and Substance Abuse Hospitals

This industry comprises establishments known and licensed as psychiatric and substance abuse hospitals primarily engaged in providing diagnostic, medical treatment, and monitoring services for inpatients who suffer from mental illness or substance abuse disorders. The treatment often requires an extended stay in the hospital. These establishments maintain inpatient beds and provide patients with food services that meet their nutritional requirements. They have an organized staff of physicians and other medical staff to provide patient care services.

Psychiatric, psychological, and social work services are available at the facility. These hospitals usually provide other services, such as outpatient services, clinical laboratory services, diagnostic X-ray services, and electroencephalograph services.

Cross-References

- Establishments primarily engaged in providing treatment of mental health and substance abuse illnesses on an exclusively outpatient basis are classified in Industry 621420, Outpatient Mental Health and Substance Abuse Centers;
- Establishments referred to as hospitals but primarily engaged in providing inpatient treatment of mental health and substance abuse illnesses with the emphasis on counseling rather than medical treatment are classified in Industry 623220, Residential Mental Health and Substance Abuse Facilities; and
- Establishments referred to as hospitals but primarily engaged in providing residential care for persons with intellectual and developmental disabilities are classified in Industry 623210, Residential Intellectual and Developmental Disability Facilities.

6223 Specialty (except Psychiatric and Substance Abuse) Hospitals 622310 Specialty (except Psychiatric and Substance Abuse) Hospitals

This industry comprises establishments known and licensed as specialty hospitals primarily engaged in providing diagnostic and medical treatment to inpatients with a specific type of disease or medical condition (except psychiatric or substance abuse). Hospitals providing long- term care for the chronically ill and hospitals providing rehabilitation, restorative, and adjustive services to physically challenged or disabled people are included in this industry. These establishments maintain inpatient beds and provide patients with food services that meet their nutritional requirements. They have an organized staff of physicians and other medical staff to provide patient care services. These hospitals may provide other services, such as outpatient services, diagnostic X-ray services, clinical laboratory services, operating room services, physical therapy services, educational and vocational services, and psychological and social work services.

Cross-References

- Establishments known and licensed as hospitals primarily engaged in providing diagnostic and therapeutic inpatient services for a variety of medical conditions, both surgical and nonsurgical, are classified in Industry 622110, General Medical and Surgical Hospitals;
- Establishments known and licensed as hospitals primarily engaged in providing diagnostic and treatment services for inpatients with psychiatric or substance abuse illnesses are classified in Industry 622210, Psychiatric and Substance Abuse Hospitals;
- Establishments referred to as hospitals but primarily engaged in providing inpatient nursing and rehabilitative services to persons requiring convalescence are classified in Industry 623110, Nursing Care Facilities (Skilled Nursing Facilities);
- Establishments referred to as hospitals but primarily engaged in providing residential care of persons with intellectual and developmental disabilities are classified in Industry 623210, Residential Intellectual and Developmental Disability Facilities; and
- Establishments referred to as hospitals but primarily engaged in providing inpatient treatment for mental health and substance abuse illnesses with the emphasis on counseling rather than medical treatment are classified in Industry 623220, Residential Mental Health and Substance Abuse Facilities.

623 Nursing and Residential Care Facilities

Industries in the Nursing and Residential Care Facilities subsector provide residential care combined with either nursing, supervisory, or other types of care as required by the residents. In this subsector, the facilities are a significant part of the production process, and the care provided is

a mix of health and social services with the health services being largely some level of nursing services.

6231 Nursing Care Facilities (Skilled Nursing Facilities)

62311 Nursing Care Facilities (Skilled Nursing Facilities) 623110 Nursing Care Facilities (Skilled Nursing Facilities)

This industry comprises establishments primarily engaged in providing inpatient nursing and rehabilitative services. The care is generally provided for an extended period of time to individuals requiring nursing care. These establishments have a permanent core staff of registered or licensed practical nurses who, along with other staff, provide nursing and continuous personal care services.

Illustrative Examples

- Convalescent homes or convalescent
- Hospitals (except psychiatric)
- Nursing homes
- Rest homes with nursing care
- Assisted living facilities (without nursing facilities) for the elderly with nursing care
- Inpatient care hospices

Cross-References

- Assisted living facilities with on-site nursing care facilities are classified in U.S. Industry 623311, Continuing Care Retirement Communities; and
- Psychiatric convalescent homes and other establishments primarily engaged in providing inpatient treatment of mental health and substance abuse illnesses with an emphasis on counseling rather than medical treatment are classified in Industry 623220, Residential Mental Health and Substance Abuse Facilities.

6232 Residential Intellectual and Developmental Disability, Mental Health, and Substance Abuse Facilities

This industry group comprises establishments primarily engaged in providing residential care (but not licensed hospital care) to people with intellectual and developmental disabilities, mental illness, or substance abuse problems.

623210 Residential Intellectual and Developmental Disability Facilities

This industry comprises establishments (e.g., group homes, hospitals, intermediate care facilities) primarily engaged in providing residential care services for persons with intellectual and developmental disabilities. These facilities may provide some health care, though the focus is room, board, protective supervision, and counseling.

Cross-References

- Establishments primarily engaged in providing inpatient treatment of mental health and substance abuse illnesses with an emphasis on counseling rather than medical treatment are classified in Industry 623220, Residential Mental Health and Substance Abuse Facilities;

- Establishments primarily engaged in providing treatment of mental health and substance abuse illnesses on an exclusively outpatient basis are classified in Industry 621420, Outpatient Mental Health and Substance Abuse Centers;
- Establishments known and licensed as hospitals primarily engaged in providing inpatient treatment of mental health and substance abuse illnesses with an emphasis on medical treatment and monitoring are classified in Industry 622210, Psychiatric and Substance Abuse Hospitals; and
- Establishments primarily engaged in operating group homes for the hearing or visually impaired are classified in Industry 623990, Other Residential Care Facilities.

623220 Residential Mental Health and Substance Abuse Facilities

This industry comprises establishments primarily engaged in providing residential care and treatment for patients with mental health and substance abuse illnesses. These establishments provide room, board, supervision, and counseling services. Although medical services may be available at these establishments, they are incidental to the counseling, mental rehabilitation, and support services offered. These establishments generally provide a wide range of social services in addition to counseling.

Illustrative Examples

- Alcoholism or drug addiction rehabilitation
- facilities (except licensed hospitals)
- Psychiatric convalescent homes or hospitals
- Mental health halfway houses
- Residential group homes for the emotionally disturbed

Cross-References

- Establishments primarily engaged in providing treatment of mental health and substance abuse illnesses on an exclusively outpatient basis are classified in Industry 621420, Outpatient Mental Health and Substance Abuse Centers;
- Establishments primarily engaged in providing residential care for persons with intellectual and developmental disabilities are classified in Industry 623210, Residential Intellectual and Developmental Disability Facilities;
- Establishments known and licensed as hospitals primarily engaged in providing inpatient treatment of mental health and substance abuse illnesses with an emphasis on medical treatment and monitoring are classified in Industry 622210, Psychiatric and Substance Abuse Hospitals; and
- Establishments primarily engaged in operating halfway group homes for delinquents and ex-offenders are classified in Industry 623990, Other Residential Care Facilities.

62331 Continuing Care Retirement Communities and Assisted Living Facilities for the Elderly

This industry comprises establishments primarily engaged in providing residential and personal care services for (1) the elderly and other persons who are unable to fully care for themselves and/or (2) the elderly and other persons who do not desire to live independently. The care typically includes room, board, supervision, and assistance in daily living, such as housekeeping services. In some instances, these establishments provide skilled nursing care for residents in separate on-site facilities.

Illustrative Examples

- Assisted living facilities with on-site nursing care facilities
- Continuing care retirement communities
- Assisted living facilities for the elderly without nursing care
- Rest homes without nursing care

Cross-References

- Establishments primarily engaged in providing inpatient nursing and rehabilitative services are classified in Industry 62311, Nursing Care Facilities (Skilled Nursing Facilities); and
- Apartment or condominium complexes where people live independently in rented housing units are classified in Industry 53111, Lessors of Residential Buildings and Dwellings.

623311 Continuing Care Retirement Communities

This U.S. industry comprises establishments primarily engaged in providing a range of residential and personal care services with on-site nursing care facilities for (1) the elderly and other persons who are unable to fully care for themselves and/or (2) the elderly and other persons who do not desire to live independently. Individuals live in a variety of residential settings with meals, housekeeping, social, leisure, and other services available to assist residents in daily living. Assisted living facilities with on-site nursing care facilities are included in this industry.

Cross-References

- Establishments primarily engaged in providing inpatient nursing and rehabilitative services are classified in Industry 623110, Nursing Care Facilities (Skilled Nursing Facilities);
- Assisted living facilities without nursing care are classified in U.S. Industry 623312, Assisted Living Facilities for the Elderly; and
- Apartment or condominium complexes where people live independently in rented housing units are classified in Industry 531110, Lessors of Residential Buildings and Dwellings.

623312 Assisted Living Facilities for the Elderly

This U.S. industry comprises establishments primarily engaged in providing residential and personal care services without nursing care for (1) the elderly or other persons who are unable to fully care for themselves and/or (2) the elderly or other persons who do not desire to live independently. The care typically includes room, board, supervision, and assistance in daily living, such as housekeeping services.

Illustrative Examples

- Assisted living facilities for the elderly without nursing care
- Rest homes without nursing care

Cross-References

- Assisted living facilities with on-site nursing care facilities are classified in U.S. Industry 623311, Continuing Care Retirement Communities;
- Assisted living facilities for the elderly with nursing care or rest homes with nursing care are classified in Industry 623110, Nursing Care Facilities (Skilled Nursing Facilities); and

- Apartment or condominium complexes where people live independently in rented or owned housing units are classified in Industry 531110, Lessors of Residential Buildings and Dwellings.

623990 Other Residential Care Facilities

This industry comprises establishments primarily engaged in providing residential care (except residential intellectual and developmental disability facilities, residential mental health and substance abuse facilities, continuing care retirement communities, and assisted living facilities for the elderly). These establishments also provide supervision and personal care services.

Illustrative Examples

- Boot or disciplinary camps (except correctional) for delinquent youth
- Group homes for the hearing or visually impaired
- Child group foster homes
- Delinquent youth halfway group homes
- Halfway group homes for delinquents or ex-offenders
- Homes for unwed mothers
- Group homes for the disabled without nursing care
- Orphanages

Cross-References

- Residential intellectual and developmental disability facilities are classified in Industry 623210, Residential Intellectual and Developmental Disability Facilities;
- Continuing care retirement communities are classified in U.S. Industry 623311, Continuing Care Retirement Communities;
- Residential mental health and substance abuse facilities are classified in Industry 623220, Residential Mental Health and Substance Abuse Facilities;
- Assisted living facilities for the elderly without nursing care are classified in U.S. Industry 623312, Assisted Living Facilities for the Elderly;
- Establishments primarily engaged in providing inpatient nursing and rehabilitative services are classified in Industry 623110, Nursing Care Facilities (Skilled Nursing Facilities);
- Establishments primarily engaged in providing temporary shelter are classified in U.S. Industry 624221, Temporary Shelters;
- Privately operated correctional facilities are classified in Industry 561210, Facilities Support Services; and
- Government operated correctional facilities and camps are classified in Industry 922140, Correctional Institutions.

Suggested citation: Lynn, S. (2023). Texas Critical Infrastructure Healthcare Supply Chain Protection. *One Step Ahead,* April 2023, 32-55.

The Institute for Homeland Security

Future Topics in Research

Criminal Threats, Emergency and Mental Depression Detection and Response on Mining Social Media

Malware Detection Using Deep Learning with Hybrid Malware Features

Workplace Harassment and Violence

Drones and Port Security at the Port of Brownsville.

Cyber-Security Threat: Benchmarking Cybersecurity Response Procedure for Hospitals in Texas

SWIR - Based object/Human Recognition and Abnormal Detection for Critical Infrastructure Protection

Countering Workplace Violence (WPV) in healthcare

Forensic Digital Data Sanitization

Assessing and Bolstering Critical Energy Infrastructure Security Using Geo-spatial Technologies.

Crossing Borders: An Analysis of Supply Chain Risks and Best Practices at the US/Mexico Border

Examining Use Cases for Drones (UAS/RPAS) at the Texas Medical Center

Supply Chain Risks of Illicit Trade in Counterfeit Pharmaceuticals

For More Information on Events, Training or Research Opportunities find us at ihsonline.org

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Criminal Justice Center
SAM HOUSTON STATE UNIVERSITY
MEMBER THE TEXAS STATE UNIVERSITY SYSTEM