INSTITUTE FOR HOMELAND SECURITY

The Transformation of Security in the Texas Energy Sector
"The CSO and CISO Convergence Survey"

Justen R. Noakes

Sam Houston State University

MEMBER THE TEXAS STATE UNIVERSITY SYSTEM

Contents

Acknowledgements 1

Abstract / Introduction 2

Introduction 3

Problem Statement and Discussion 5

The Way Forward 6

The Survey 7

Survey Findings 8

Conclusion 9

Survey Questions and Answers 10

References 13

Author Biography 14

Acknowledgements

I want to express my sincere thanks and gratitude to the team at the Institute of Homeland Security at Sam Houston State University for their continued support of this vital research and my professional development, specifically Rob Crane, Michael Aspland, Shannon Lane, Grant Threatt, Reyna Loosmore, John Suarez, Heberto Villarreal, Scott Lynn, and Clyde Loll.

I would also like to thank the following individuals and their agencies for their support and contributions to this study, including Clint Ladd, Critical Infrastructure Protection Coordinator, Texas Department of Public Safety; Byron Smith, Seven-Eleven; Daniel Nix, Executive Director, Texas AWWA; Mike Howe, Former Executive Director, Texas AWWA; Jason Knobloch, Deputy Executive Director, Texas Rural Water Association; Craig Matthews, Security Operations Team Lead, Chevron North America Exploration and Production Company; Edwin Otten, Protective Security Advisor, Cybersecurity and Infrastructure Security Agency; Mark Sloan, Homeland Security & Emergency Management Coordinator at Harris County; Joe Gleinser, Co-Founder, Chief Executive Officer at Trustgrid.

Finally, I would like to thank my family and friends, as well as Texas Search and Rescue, for their unwavering support.

Abstract / Introduction

With the security threat landscape evolving daily and the types of threats growing in complexity and frequency, the distinction between physical and cyber security is rapidly fading. Cyber criminals are stealing trillions of dollars every year and are now considered one of the biggest threats not only to companies but to humanity in totality. Given this bleak outlook, cyber criminals go nearly unscathed on the global legal playing field, with merely a fraction of a percent being apprehended, much less prosecuted. The decades-old practice of fighting cybercrimes and traditional crimes independently needs an overhaul. Understanding today's legal system is as foreign to cybersecurity experts as AI is to corporate security practitioners. Still, if there is a chance to take a bite out of cybercrimes, each one must start listening to and learning each other's languages.

As the critical infrastructure sector in the United States grapples with the evolving threat of cybercrimes, it's becoming increasingly clear that an integrated approach to security is the way forward. In an era of growing threats and evolving industry trends, critical infrastructure security has become a crucial topic in Texas governments, corporations, and organizations. The threat landscape is evolving in the critical infrastructure ecosystem, including oil, gas, the electric grid, renewables, cross-sector interdependence, and supplier relations. The need of the hour is a more integrated approach to addressing cyber, physical, and human challenges. Because of this evolution, the Chief Security Officer (CSO), the Chief Information Security Officer (CISO), or equivalent positions have become increasingly important.

This paper aims to identify the key components and needs by surveying senior executives responsible for security in Texas critical infrastructure-focused companies. These executives are increasingly concerned with security in a world driven by digital and AI trends. No longer can the practice of security be focused on "gates, guards, and guns" or simple malware and phishing attacks. With the increasing use of ransomware as a means for those seeking financial gain, as well as an act of terrorism or war by nation-state countries aiming to harm the United States, today's security professionals can no longer operate within traditional security-themed silos.

This project will survey fifty executive-level leaders in the critical infrastructure sectors in the State of Texas to help identify trends of concern in the modern-day security landscape. We will seek to understand what security topics should be addressed and how to provide practical solutions for those areas of concern. The goal is to provide modern-day security professionals with the knowledge and tools to address the convergence of traditional security practices with today's digital security demands.

Key Terms: Cybersecurity – Cyber Convergence – Digital – Energy Sector – Chief Security Officer – Chief Information Security Officer – Electrical Grid – Nation State – Terrorism – Ransomware

Introduction

Given the ever-changing landscape of security in business and industry sectors, particularly in critical infrastructure, the question arises whether corporate leadership and organizations are making changes to ensure that all security policies and incidents are transparent, proactively addressed, and seamlessly integrated across the enterprise. Or are we continuing down the traditional path of physical security professionals in neatly pressed sport coats tucked away in corporate corner offices and cyber security savants in shorts and hoodies working in dimly lit home offices? For decades, these two disciplines have rarely, if ever, interacted, much less collaborated. Convergence of the two disciplines still seems unlikely given the personalities. Still, with the skyrocketing number of cybercrimes committed each year, we must learn to work collectively and proactively to better protect the interests of not only our business but the United States as a whole.

In recent history, the term “security” in the business community typically referred to “guards, gates, and guns,” focusing on protecting executives and employees and assets from workplace violence, outsider threats, and retail theft. Over the last decade, the identity of the security professional has started to evolve from the traditional definition to include digital and data security. This trade was initially begun to protect digital environments from phishing attacks, viruses, and malware, but has since evolved into a multi-billion-dollar corporate cornerstone. When referring to the term “security”, today’s Google search returns many more examples of cyber-related topics than physical security-related topics, and as we will learn, for good reason.

Cybersecurity started in 1971 when Bob Thomas, a computer programmer with Cambridge research thinktank BBN (Bolt, Beranek and Newman, Inc.), created and deployed a virus that served as a security test. The virus was named “Creeper” after a Scooby Doo villain. It was designed to move across ARPANET (Advanced Research Projects Agency Network), which was established by the U.S. Department of Defense and was the forerunner of the internet. The computer worm was intended to be a non-harmful, self-replicating experimental program, intended to illustrate how mobile applications work. However, it corrupted the DEC PDP-10 mainframe computers at the

Digital Equipment Corporation, interfering with the teletype computer screens that were connected. All the users could see on the screen were the words “I’m the creeper, catch me if you can!”

In response, Ray Tomlinson, Thomas’ colleague, created the Reaper Program. It was similar to the Creeper in that it moved through the internet, replicating itself, and finding copies of the Creeper, logging them out to render them ineffective. The Reaper was the first attempt at cybersecurity – the first antivirus software program.

As cyber-attacks have evolved, so has cybersecurity. Much like physical security, as adversarial forces work methodically to grow and become more sophisticated in an attempt to thwart defense measures, hackers work tirelessly every day to poke holes in corporate cybersecurity countermeasures and defense structures.

Through the 80s and 90s, almost as fast as the internet evolved, so did cyber-attacks. The first significant attack on the Internet occurred in 1988, even before the World Wide Web made its public debut.

At the turn of the century, there were more sophisticated attacks and an abundance of advanced persistent threat actors (APTs), most of which were sponsored by nation-states. The evolution of cybercrime led to the emergence of new viruses and worms, causing significant damage to critical sectors of the global digital economy. By decade’s end, cybersecurity was a concern to computer users everywhere, but especially to government agencies and large corporations who had the most at stake.

As cybercrime was finding its footing in the 2010s, the past decade has seen the ecosystem develop in new ways. There has been a rise in cybercrime driven by technological advances as well as socioeconomic forces, particularly in Eastern Europe and Asia. As organizations rapidly digitize, turning to the cloud, individual endpoints, and global expansion, they are doing so faster than their cybersecurity measures can keep up.

In the past 50 years, the advancement of cybercrime across the globe has resulted in:

- Cybercrime is the number one global business risk
- The average cost of a data breach is now $4.45 million
- 82% of breaches involve the cloud
- Healthcare is the top-attacked industry
- Phishing and compromised credentials are the top two attack vectors
- Ransomware made up 24% of attacks in 2023

Problem Statement and Discussion

It's clear that cybercrime has evolved rapidly, and while advances in cybersecurity continue to happen, it's a constant battle between overworked, understaffed information security departments and threat actors.

We expect global cybercrime damage costs to grow by 15% this year, reaching $10.5 trillion by the end of 2025, up from $3 trillion in 2015. This represents the most significant transfer of economic wealth in history, exponentially surpassing the damage caused by natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined. If it were measured as a country, then cybercrime would be the world's third-largest economy after the U.S. and China.

By comparison, traditional retail theft has long been the focus of corporate security departments for decades. In 2023, a survey collected responses from 177 retail brands across 28 different retail sectors, including apparel, jewelry, grocery, and department stores, and accounted for more than 97,000 retail locations and $1.6 trillion in annual retail sales. Shrink for total retail sales in 2022 reached $112.1 billion, up from $93.9 billion in losses in 2021, according to the survey. Even at topping over one hundred billion dollars in losses, this long-standing security focal point pales in comparison to the trillions of dollars being lost each year in the cyber arena.

As theft continues to march on at a steady pace, spending to combat this form of robbery continues along with it. The global retail loss prevention market is estimated to be valued at approximately $24.5 billion in 2023 and is anticipated to reach around $47.1 billion by 2033. Retailers spend roughly $12 billion annually on theft prevention measures. Again, in comparison to cybercrime prevention, the money and resources spent on traditional theft are nearly a quarter of those spent on cybercrime prevention.

Global security spending will reach $219 billion this year and grow to nearly $300 billion in 2026, according to an IDC forecast released Thursday. Investments in cybersecurity software, hardware, and services will outperform growth in overall IT spending.

The largest spenders on information security this year will include organizations in banking, manufacturing, professional services, and the federal government. The four industries will account for more than one-third of all security spending this year, according to IDC.

The exact numbers vary massively depending on how you choose to define an attack, but according to estimates by Microsoft, there are 600 million cyberattacks per day.

The Identity Theft Resource Center (ITRC) Annual Data Breach Report recorded 3,205 cyberattacks leading to data compromises in 2024. This marks an increase from 2,365 in 2023, 1,584 in 2022, and just 754 in 2018. That's approximately 8.7 attacks per day.

However, the number of victims is substantially higher at over 1.7 billion per year. That's more than 4.6 million per day, or nearly 54 per second.

Billionaire businessman and philanthropist Warren Buffet calls cybercrime the number one problem with mankind and cyberattacks a bigger threat to humanity than nuclear weapons. There is squarely a bullseye on our nation's businesses. According to a 2024 Sophos study, 59% of companies were hit by ransomware in the last 12 months. That's a drop from a high of 66% in each of the previous two years.

Organized cybercriminal entities are joining forces, and their likelihood of detection and prosecution is estimated to be as low as 0.05 percent in the U.S., according to the World Economic Forum's 2020 Global Risk Report.

That means that if we use the ITRC Annual Data Breach Report, which recorded 3,205 cyberattacks leading to data compromises in 2024, as our baseline, then only one case would have been prosecuted. With the introduction of the Creeper virus well over fifty years ago, the extreme proliferation of cybercrimes, and the enormous amounts of money being lost and spent, the lack of ability to apprehend and prosecute cybercriminals remains a challenge. Some of the difficulties associated with prosecuting cybercrimes include jurisdictional challenges, identification of the offender, resources to arrest and prosecute the offender, and the legal mechanisms to convict the offender. Given these challenges, the burden of prevention falls squarely on the businesses most impacted by these crimes.

The Way Forward

To better equip security professionals and facilitate the prosecution of cybercrimes, there is a growing trend in critical infrastructure businesses to converge the fields of physical and cyber security. Theoretically, this would be very beneficial for both trades, allowing those in physical security to have greater access to technology professionals, and giving cybersecurity teams access to well-established, connected security experts who know how to navigate the legal and criminal landscape. This would include consolidating security policy and enforcement under a single enterprise authority.

With a conviction rate of less than one percent, cybersecurity experts are rightfully focused on the defensibility of the systems they are responsible for, rather than pursuing the cybercriminal. Cybersecurity experts rarely have classical security or law enforcement experience, knowledge, or training, as they typically tend to enter the cybersecurity workspace from technology-centric lines of work. Due to this gap in

knowledge and with a team of technology-focused individuals, most cybersecurity departments lack the expertise or desire to pursue legal action against perpetrators of cybercrimes.

Theoretically, merging physical security and cyber security departments would allow for the cross-pollination of best practices, shared relationships, and established protocols, benefiting both groups, as well as giving them more capabilities to prevent criminal incidents and pursue criminals. However, due to the significant differences in work and personality types, the adoption of the convergence has been slow.

The Survey

To better understand the adoption of convergence between the two security departments by businesses in the critical infrastructure, the CSO and CISO Convergence Survey presents fourteen questions to senior leaders to understand how their physical security and cyber security departments interact. The questions are divided into three groups: four questions will help establish survey-taker demographics. The next set of nine questions aims to better understand the current level of interaction between the two security departments, and a final question will determine if the company has already merged the departments or plans to do so.

The survey audience was intended to be senior leadership with oversight of one or both of the security departments. The survey was administered online through the Institute of Home Security at Sam Houston State University, specifically to professional organizations across the state. The organizations who participated included the Energy Security Council, Private Sector Advisory Council, Texas American Water Works Association, Texas Rural Water Association, Texas Water/Wastewater Agency Response Network (TXWARN), Water Environment Association of Texas (WEAT), South Texas Oilfield Crime Committee, Permian Basin Oilfield Crime Committee (PBOCC), and Oilfield Theft Intelligence Sharing (OTIS).

There were fifty-nine total survey responses, sixteen of which were not complete, resulting in a total of forty-three complete surveys. All forty-three complete responses were used for the survey results.

Survey Findings

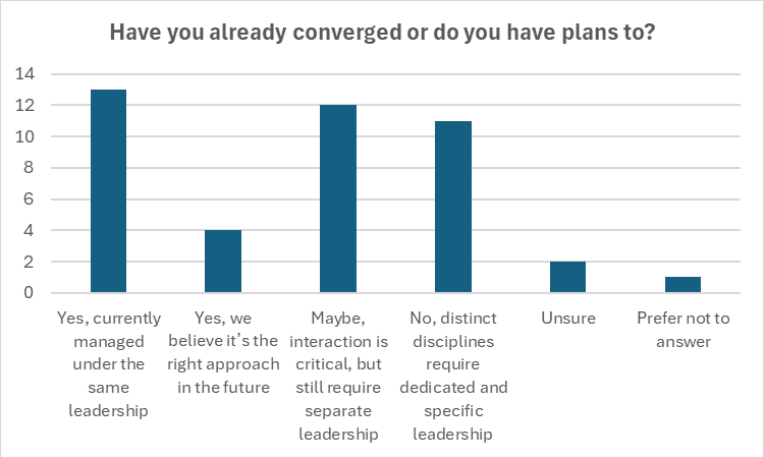
The first four questions of the survey are about survey participant demographics, including title, size of company, tenure, and whether they considered security as part of their job responsibility. The survey respondents were mainly from smaller organizations, with roughly one-third (15 of 43 responses) working for companies with fewer than 50 employees and half of the responses from companies with fewer than 500 employees (22 of 43 responses). By definition from the Small Business Administration, any business with fewer than 500 employees is considered a small business. Due to the lower number of employees, small business owners and leaders tend to wear many hats and perform multiple administrative roles within an organization, which may account for some of the security duties already converged. Fifteen respondents were from larger companies with 1,000 or more employees. Of those fifteen companies, about half (8 of 15 responses) believed it would be beneficial to combine the duties and had already done so or were planning to converge. One important note is that nearly all respondents believed that security was part of their job responsibilities. Job tenure was evenly distributed throughout the group, representing a good mix of experience.

Questions five through thirteen review how security departments work with each other during specific incident types, as well as how threats are perceived in the organization. When asked to rank different types of security and what they considered the word “security” to mean, they chose phishing attacks and ransomware, 84% and 80% respectively, over physical attacks such as active shooters and civil unrest. Although nearly every respondent considered security as part of their job responsibilities, fewer than half reported thinking about security, both physical and cyber, on a daily basis.

Although the convergence does not appear to be taking place from a department leadership perspective, it does seem that leaders from both departments are working together when there is a kinetic or cyber incident. A majority of leaders in the physical security department, 33 of 43 respondents, are either directly involved or at least aware of any cyber incidents. There is also broad adaptation in that both disciplines are represented on the company's emergency response teams to a great extent, with 37 of the 43 respondents convening both departments during large-scale disasters. Another good sign of convergence from an operational perspective is that over two-thirds of the companies participate in both cyber and physical exercises and training, and nearly half (20 of 43 responses) of the companies house both departments in the same building. However, that may be more of a direct reflection of the company size than convergence.

Conclusion

Despite the staggering numbers associated with cybercrimes, particularly the daily amount of money being stolen, there remains a significant gap in our ability to defend against, catch, and prosecute cybercriminals, compared to our capacity to complete the legal cycle for traditional crimes. Yes, there are numerous factors contributing to the difficulty in capturing cyber criminals, but given their impact, leveraging existing experts in the criminology field seems like a logical starting point. To that point, some businesses have already made the convergence with both departments reporting to the same leader; roughly one-third of the leaders surveyed had already made the convergence. However, this means that roughly two-thirds of the survey respondents are undecided or do not believe that convergence is part of their future.



The survey responses also indicate that there is still a strong desire, or belief, that the two disciplines are very distinct and require different leadership. Although it does not appear that convergence is a top organizational priority for company leadership, from an operations perspective, both departments seem to work together when issues arise on both sides of the fence. Based on the survey, it also appears that there is a good amount of collaborative training and situational awareness. So, regardless of whether organizational convergence occurs or not, there does appear to be collaboration between both cyber and physical security departments, which, if it holds, those companies and organizations that have not yet brought the two together will likely be forced to do so out of necessity in the near future.

Survey Questions and Answers

The following are the questions and answer options that were presented as part of the survey.

1. What is your current job title?
    a. CEO (Chief Executive Officer) 6
    b. CISO (Chief Information Security Officer) 2
    c. CSO (Chief Security Officer) 6
    d. COO (Chief Operating Officer) 0
    e. Other Executive or Managerial Position 29

2. What is the total number of employees at your company?
    a. Less than 50 15
    b. 51 - 100 3
    c. 101 - 500 4
    d. 501 - 1,000 6
    e. 1,001 - 5,000 9
    f. 5,001 - 10,000 1
    g. More than 10,000 5

3. How many years have you been in your current position?
    a. Less than 1 year 5
    b. 1 - 3 years 8
    c. 4 - 5 years 6
    d. 6 - 10 years 9
    e. 11 - 15 years 6
    f. More than 15 years 9

4. Do you consider safety and/or security to be part of your job responsibilities?
    a. Yes 41
    b. Partially 2
    c. No 0

5. When thinking about 'security' at your workplace, rate the following terms.

Field	Min	Max	Mean
Active Shooter	5.00	100.00	63.15
Phishing Attack	40.00	100.00	84.50
Ransomware	4.00	100.00	80.55
Theft	10.00	100.00	61.37
Civil Unrest	0.00	100.00	41.18

6. When thinking about a typical day at work, how often do you worry about physical security? (workplace violence, active shooter, criminal acts, etc.)
    a. Daily.....18
    b. Several times a week.....5
    c. Occasionally during the week.....9
    d. Rarely 8
    e. Never 2
    f. I would prefer not to answer 1

7. When thinking about a typical day at work, how often do you worry about a cyber incident? (data breach, ransomware, network attack, etc.)
    a. Daily.....20
    b. Several times a week.....4
    c. Occasionally during the week.....16
    d. Rarely 3
    e. Never 0
    f. I would prefer not to answer 0

8. How is your company's physical and cyber security leadership organized?
    a. Both report to the same C-suite leader and the same senior leader. 20
    b. Both report to the same C-suite leader but to different senior leaders. 9
    c. They report to different C-suite leaders. 9
    d. I am unsure. 3
    e. I prefer not to answer. 2

9. During a response to a cyber incident, how involved is your physical security leadership?
    a. They are deeply involved. 14
    b. They are aware of the incident and are involved in the response. 14
    c. They are aware of the incident, not directly involved in the response. 8
    d. They are not involved in any aspect of the response. 1
    e. I am unsure. 4
    f. I prefer not to answer. 2

10. Where are your physical and cyber security departments located?
    a. They are co-located in the same department or on the same floor. 10
    b. They are co-located in the same building. 11
    c. They are located on the same campus. 7
    d. They are not located near each other. 10
    e. I am unsure of their location. 3
    f. I prefer not to answer. 2

11. Do you convene both physical and cyber security leaders when a natural or significant man-made disaster occurs?

    a. Yes, they are both part of our emergency response team. 28
    b. Yes, but only the affected business unit is involved. 7
    c. No, we allow them to manage the incident independently. 3
    d. I am unsure. 3
    e. I prefer not to answer. 2

12. Do members of the cyber security team participate in training and exercises conducted by the physical security team?

    a. Yes, our departments are integrated, so we collectively participate in all training and exercises. 19
    b. Yes, but only when it pertains to areas of the business we are responsible for. 6
    c. Yes, but only as observers or third parties. 3
    d. No, we do not participate in any training or exercises together. 13
    e. I am unsure. 0
    f. I prefer not to answer. 2

13. Do members of the physical security team participate in training and exercises conducted by the cybersecurity team?

    a. Yes, our departments are integrated, so we collectively participate in all training and exercises. 14
    b. Yes, but only when it pertains to areas of the business we are responsible for. 11
    c. Yes, but only as observers or third parties. 2
    d. No, we do not participate in any training or exercises together. 11
    e. I am unsure. 2
    f. I prefer not to answer. 3

14. Do you have plans or envision a time when the physical security and cyber security departments would be managed under the same leadership?

    a. Yes, they are currently managed under the same leadership at our company. 13
    b. Yes, we believe it's the right approach and plan to implement it in the future. 4
    c. Maybe—while we believe the interaction between the two departments is critical, they still require separate leadership. 12
    d. No, these departments are distinct disciplines that require dedicated and specific leadership. 11
    e. I am unsure. 2
    f. I prefer not to answer. 1

References

Arctic Wolf. (04/19/2024). A Brief History of Cybercrime, Take a look at the history of cybercrime, the most devastating cyber attacks seen to date, along with rundowns of the fallout. https://arcticwolf.com/resources/blog/decade-of-cybercrime

Identity Theft Resource Center. (2024). ITRC 2024 Annual Data Breach Report. https://www.idtheftcenter.org/publication/2024-data-breach-report

Kapko, M. (03/17/2023). Global cybersecurity spending to top $219B this year: IDC. *Cybersecurity Dive.* https://www.cybersecuritydive.com/news/cybersecurity-spending-increase-idc/645338/#:~:text=According%20to%20an%20IDC%20forecast%2C%20global%20cybersecurity,*%20Increased%20data%20privacy%20and%20governance%20regulations

Martin, J. (06/06/2025). How Many Cyber Attacks Occur Each Day? *Exploding Topics*. https://explodingtopics.com/blog/cybersecurity-stats

Monroe University. Cybersecurity History: Hacking & Data Breaches. https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches

Morgan, S. (11/05/2024). Boardroom Cybersecurity Report 2024, 25 cybercrime facts, figures, predictions, and statistics for C-Suite executives. *Secureworks.* https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024

Olson, C. (09/26/2023). 'Unprecedented' theft contributed to $112 billion in retail losses last year. *Los Angeles Times*. https://www.seattletimes.com/business/unprecedented-theft-contributed-to-112-billion-in-retail-losses-last-year/

Sophos. (06/2025). The State of Ransomware 2025. https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-ofransomware-2024-wp.pdf

World Economic Forum. (2020). The Global Risks Report. https://www.weforum.org/publications/the-global-risks-report-2020

Author Biography

Mr. Justen R. Noakes is the President/CEO of KTLO Solutions, a professional consulting firm that provides enterprise risk management solutions focused on business and industry. Mr. Noakes has over thirty years of retail experience in engineering, project management, information technology, and emergency management. Mr. Noakes developed and led the Emergency Preparedness Department for H-E-B from 2004 to 2024. In those twenty years, Mr. Noakes led H-E-B's response to over twenty presidential-declared disasters, most notably Hurricanes Rita, Ike, and Harvey, as well as the COVID-19 Pandemic and Winter Storm Uri in 2021. Mr. Noakes serves as the Executive Director for BeforeDuringAfter, a non-profit that provides free business resilience solutions for small businesses. Mr. Noakes previously served on the Board of Directors for Texas Search and Rescue, an all-volunteer first responder organization, and as a Bexar County ESD2 Fire Department Commissioner. Mr. Noakes currently serves on the Texas Emergency Management Advisory Council at the request of the Governor.

Disclosure statement:
The author of this technical report, pertaining to the granted project, hereby discloses that there exist no conflicts of interest or competing interests to declare in relation to the research, authorship, and publication of this work.

INSTITUTE FOR HOMELAND SECURITY

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, Public Health, Water and Wastewater.

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.

Institute For Homeland Security
Sam Houston State University

Noakes, J. (2026). The Transformation of Security in the Texas Energy Sector “The CSO and CISO Convergence Survey”. (Institute for Homeland Security Report No. 2026-1033).
Institute for Homeland Security.