INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

ENSURING THE CYBERSECURITY OF TEXAS' CRITICAL INFRASTRUCTURES

Institute for Homeland Security

Sam Houston State University

Brooke Nodeland

Ensuring the Cybersecurity of Texas' Critical Infrastructures Brooke Nodeland

Abstract:

The daily threat of cyber-attacks on Texas' critical infrastructure present significant challenges for public and private critical infrastructure providers. COVID-19 related supply chain issues provided insight into the catastrophic effects that could be caused by a cyber-attack on the transportation sector. These disruptions effect our ability to distribute products and medical necessities as well as essential personnel in times of crisis. Protecting the state's transportation, energy, and chemical cyber networks is imperative in ensuring the sustainability of daily life and business continuity in the event of a cyber-attack. Of additional concern is a growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems creating ample opportunities for exploitation of the transportation cyber systems on which industry have become dependent (Transportation Systems Sector-Specific Plan, 2015). The cyber security of the energy sector ensures the health and welfare of Texans by ensuring steady energy is supplied via electricity, oil and other natural gas resources. The energy infrastructure is primarily owned in the private sector, supplies fuel to the transportation industry, and electricity to businesses and households. Recent ransomware attacks aimed at Western targets, including the energy sector, continue to pose challenges in cybersecurity (Montague, 2023). The recent accidental chemical spill in Ohio also provides insight into the possible outcomes of an intentional cyber-attack against this infrastructure. The regular operations of the chemical sector are imperative to the economic and manufacturing health of state and often involves transporting dangerous chemicals on which other critical infrastructures are dependent (Introduction to the Chemical Sector Risk Management Agency, n.d.).

Cyber threats are of particular concern in Texas, where large corporations continue to relocate, and the population continues to climb. It is imperative industry leaders are able to recognize and identify their cyber risks to develop prevention strategies and respond to cyberattacks more quickly and effectively. Disruptions to critical infrastructures could lead to theft of intellectual property; supply chain disruption; electricity disruption; loss of operations capacity; or chemical theft, diversion, or release (Introduction to the Chemical Sector Risk Management Agency, n.d.). Texas' industrial vulnerability to cyber-attacks through phishing, ransomware, and malware pose significant threats to the security of critical infrastructures. Securing networks

against internal and external cyber-attacks requires industry leaders to be proactive and reactive in their approach. The proposed paper seeks to present a translational synthesis of the existing literature regarding best cybersecurity practices for securing critical infrastructure in Texas. In doing so, agencies will be able to better align and prioritize cybersecurity initiatives with industry missions, risk tolerance, and resources (Cybersecurity, C.I., 2018). This review will also include recommendations for improving risk readiness for the transportation, energy, and chemical industry in the state moving forward.

Keywords: cybersecurity, transportation, energy, chemical, critical infrastructur

Introduction and overview

Nearly 25 years ago, the attention of the nation was on the terrorist attacks on September 11, 2001, and in the days that followed, society seemed to virtually shut down. The physical attacks on the World Trade Center were unprecedented in American history and fueled national discussion of the security of the nation's critical infrastructures. The following month, President Bush convened the President's National Infrastructure Advisory Council (NIAC) by executive order whose responsibility since has been to advise the President on practical strategies for industry and government to reduce complex risks to critical infrastructures. The following year, the Department of Homeland Security (DHS) became a formal stand-alone federal department to coordinate and unify national homeland security efforts (Creation of the Department of Homeland Security, n.d.). In the years since, the council's, DHS, and national conversation has extended beyond simply the prevention of physical attacks on critical infrastructure, to ensuring protection and response plans for cyber-attacks on these important assets.

The national Cybersecurity and Infrastructure Security Agency (CISA), part of the DHS, was created by President Trump in 2018. The mission of the cybersecurity division is to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense, resilience of national critical functions, and a robust technology ecosystem (Cybersecurity Division, n.d.). To accomplish this, CISA works to fortify the nation's cyber defenses against immediate threats and vulnerabilities, building the nation's long-term capacity to withstand and operate through cyber incidents, to achieve a defensible cyberspace ecosystem by ensuring that changes in the ecosystem shift the advantage to network defenders (Cybersecurity Division, n.d.). They are responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the governments cybersecurity against both private and nation-state hackers (Cimpanu, 2018). CISA makes critical infrastructure designations because their assets, systems, and networks, both physical and virtual, are considered to be so vital to the United States that their incapacitation or destruction would debilitate the security, national economic security, national public health or safety or some combination, of the entire country (Gregory, 2022). Further, when a cyber-attack occurs against one of these assets, the impact typically goes beyond the direct industrial fall-out by way of a ripple effect with many often-unexpected consequences (Gregory, 2022). The

transportation systems sector, chemical sector, and energy sector are among the 16 critical infrastructures in the U.S.

Recent events, such as the novel coronavirus COVID-19 pandemic, provide some insight into what the real-world impact could be if a cyber-attack against critical infrastructure occurred. By mid-2020, the COVID-19 pandemic had significantly impacted the daily lives of people and businesses around the world as the result of mandatory shutdowns and stay at home orders for millions of Texans and Americans (Ivanov & Dolgui, 2020). These orders forced workers out of offices and into work from home situations, for those who were able to keep their jobs, with essential workers comprising those who were leaving the house. These shutdowns had a profound impact on almost every aspect of daily life, including the creation of significant new opportunities for cyber criminals (Kumar, Sharma, Vachhani, & Yadav, 2022). Cyber security threats were rampant, and employees were now using their home networks to conduct business operations leaving ample opportunity for cyber breaches (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple, & Bellekens, 2021). Further, the security of many software products were revealed to be underprepared for the drastic change in the working situations (Georgiadou, Mouzakitis, & Askounis, 2021).

According to a recent report on data breaches, cyber-attacks on critical infrastructure industries cost an average of $4.8 million, not including the cost to consumers and other businesses, such as the cost associated with supply chain disruption (Gregory, 2022). The development and deployment of the Internet of Things (IoT) has made the cyber-systems of critical assets even more susceptible attack. The primary methods of cyber-attacks to critical assets include IT failure, human error, their-party business partners, destructive attacks, ransomware, and other malicious attacks (Cost of a Data Breach Report 2023, n.d.), and typically cost more than $1 million more than other types of data breaches (Gregory, 2022). To prepare for and effectively respond to a cyber-attack, it is imperative that critical infrastructure providers understand the most prominent threats facing their cyber-networks so that they can identify their risks (Johnson, 2015). Risk assessment will allow them to work with their cyber-security team and industrial and governmental partners to develop and implement readiness and response plans to future cyber threats. Then, if, or when, a cyber-attack occurs, they are prepared with solutions that make resolution of the immediate issues and any fallout more efficient. Critical infrastructure providers are on the

frontline of defense in protecting the transportation, chemical, and energy sectors in the United States and in Texas. The following discussion presents a risk assessment for these critical infrastructures, followed by a discussion of the most prominent cyber-security threats today, and finally, an overview of strategies and recommendations for ensuring that industry leaders and government agencies are risk ready when a cyber-threat is identified.

Problem Statement

Public and private sector critical infrastructure providers face a constantly evolving landscape of increasingly destructive, and rapidly growing number of cyber-threats. Opportunities for cyber attackers have become more prevalent and more attractive as the number of devices with internet capabilities expands (Lee, 2020). The IoT technologies are comprised of computational devices that extend the connectivity of systems and users to improve and optimize real-time operations in every aspect of daily life, including power grids and industrial systems (Stellios et al., 2018). And as more information is stored and shared online, individuals, businesses, and government agencies have more to lose today than ever before (Johnson, 2015). Cyber-attackers can be anyone, including insiders like government employees or industrial employees, as well as external actors (Cormier & Ng, 2020). For example, industry insiders (e.g. poorly trained or disgruntled employees) or incompetent contractors may create opportunities for outsiders to penetrate poorly protected cyber networks and systems (Tal, 2018). Criminal organizations may target industrial cyber systems using spam, phishing, or spyware and malware, for identity theft, online fraud, or computer extortion (Tal, 2018). Cyber-attacks can be designed and targeted to damage or disrupt critical infrastructure necessary to deliver vital services by infiltrating the digital systems that control physical processes, damaging specialized equipment, and disrupting vital services without a physical attack (Johnson, 2015). If used by terrorists, nation states, or cybercriminal organizations, these attacks could destroy, incapacitate, degrade, or exploit critical infrastructures to threaten national security, weaken the economy, or cause mass casualties.

Critical infrastructure providers are typically industrial partners responsible for the management of cyber networks containing both information technology (IT) and operational technology (OT) increasing their vulnerability to cyber-threats (Ellis, Locasto, & Balenson, 2020). IT systems comprise the network of computers, servers, and mobile devices as well as the information that flows between them, by being connected to the internet; while OT includes the physical devices and software that control operations in the real world, such as meters or robotics

(5 ways to prevent cyber-attacks on critical infrastructure, n.d.). Once an OT system is compromised, the potential for threats is endless as hackers then can disrupt vital services, physically endanger employees and customers, damage or destroy equipment, and harm the environment (5 ways to prevent cyber-attacks on critical infrastructure, n.d.). **Topic Discussion**

The daily threat of cyber-attacks on Texas' critical infrastructure present significant challenges for providers in the state. Protecting the state's transportation, energy, and chemical networks is imperative to ensuring the sustainability of daily life and business continuity in the event of a physical- or cyber-attack. The states dependence on these sectors cannot be understated. Texas' transportation sector is massive, consisting of all aviation, highway and motor carriers, maritime transportation systems, mass transit and passenger rails, pipeline systems, freight rails, and postal and shipping operations, each of which have become increasingly reliant on cyberbased control, navigation, tracking, positioning, and communications systems creating ample opportunities for exploitation (Transportation Systems Sector, n.d.). Together, these subsectors are responsible for the quick, safe, and secure movement of people and goods throughout the state, and even the smallest cyber disruption can have catastrophic effects (Transportation Systems Sector, n.d.). Increasingly threats to this critical infrastructure are becoming cyber-physical, and as vehicles, aircrafts, vessels, and control systems are more often connected online, securing both the physical safety and cyber security of these assets will become synonymous (Lehto, 2020). For Texans, protecting more than 300,000 miles of highway, 10,400 miles of freight rail, nearly 400 airports, and 21 seaports, makes ensuring the cyber-security of the transportation sector an enormous operation (McPherson, Donald, & Wright, 2018).

The potential for damage inflicted by a cyber-attack can be seen in all areas of transports. For example, radio frequency technologies, such as automotive radar, are used to increase driving safety and more automated (Yeh, Choi, Prelcic, Bhat, & Heath, 2018). Autonomous vehicles are being tested and deployed (Lim & Taeihagh, 2018). Millions of passengers fly in and out of Texas each year, making aviation both vulnerable and attractive to cyber threats. Smart airports, for example, have emerged in recent years as IoT has enabled enhanced robustness, efficiency and control, and real-time monitoring and analytics of operations and cyber-security (Koroniotiset et al., 2020). While these technologies control the environmental conditions inside the airport, automate passenger-related actions, and support airport security, they also create opportunities for

security intrusions into network systems (Koroniotiset et al., 2020). While convenient, this expansion requires connectivity and data sharing across a variety of users (including customers, airline employees, external contractors, etc.) which then creates new opportunities for bad actors to infiltrate secure networks. The complexity of cyber-attacks has also increased, making smart airports more susceptible to network disruption, cancelled travel, or stealing of sensitive information (Koroniotiset et al., 2020). Consider that several times a year, one of the major airlines report significant cyber-disruption to their flight schedules causing delays and cancellations leaving thousands of passengers stranded, making them frustrated, unable to reach their destination, and resulting in significant monetary loss for customers and the airlines themselves. While the cause of these disruptions is often left out of reports, an intentional cyber-attack could cause even more damage by grounding flights, stranding passengers, making it impossible for essential personnel and cargo to be transported in the event of an emergency. Disruptions in the supply chain resulting from the novel coronavirus, COVID-19, provide just a glimpse of the potential impact of an intentional disruption to operations in the transportation sector. The pandemic led to misalignment between supply and demand, resulting from planes, trains, and maritime vessels from transporting goods in a timely or efficient manner. Delays and congestion both on land and sea lasted months, resulting in shortages in household necessities, cleaning supplies, food, as well as medical supplies, equipment, and medicines themselves. The disruption resulting from the COVID-19 fallout could be much greater if the result of an intentional, organized cyber-attack.

Relatedly, rail cars and maritime vessels often carry large amounts of hazardous materials and chemicals, and sometimes travel in very close proximity to large concentrations of people and industry, drawing attention to another critical infrastructure facing significant cyber threats (5 ways to prevent a cyber-attack on critical infrastructure, n.d.). The regular operations of the chemical sector are imperative to the economic and manufacturing health of the state and often involve transporting dangerous chemicals on which other critical infrastructures are dependent. Comprised of basic, specialty, and agricultural chemicals as well as consumer products, the chemical sector converts raw materials into diverse products that are essential to modern life (Chemical sector, n.d.). Texas is home to nearly 2,000 chemical manufacturing plants, and with Louisiana, produces

roughly 80 percent of the nation's main petrochemical supply (Texas Comptroller, n.d.). The amount of data used and produced by the industry makes it difficult to both manage and secure, placing this sector at considerable risk to cyber-threats (Texas Comptroller, n.d.). Increasingly, operational and information technologies converge to allow for remote, real-time access to the operation of chemical facilities (Cormier & Ng, 2020). The uninterrupted operation of these facilities ensures chemicals are used, manufactured, stored, transported and delivered to critical infrastructure and industrial sectors in an efficient and safe manner (Chemical sector, n.d.). The risk posed by disruption to this process was previewed in the West Fertilizer Company explosion in West, Texas in 2013, resulting in chemical fires that killed 15 and injured more than 160 people. The Colonial Pipeline ransomware attack in May 2021, provides additional insight into the potential impact of cyber-attack on this sector. The pipeline spans 5,500 miles stretching from Texas to New York and carries up to 3 million barrels of fuel per day (Gregory, 2022). In this case, hackers utilized ransomware to shut down their operations for nearly a week affecting roughly 12,000 gas stations. The shutdown reduced the amount of fuel available to the East Coast by nearly half leading to gas shortages and higher prices at the pump (Gregory, 2022). Colonial Pipeline paid $4.5 million in ransom to regain access to comprised systems and was also responsible for paying additional fines for operational lapses and management failures (Gregory, 2022). The Transportation Security Administration for U.S. pipelines also issued a series of new directives to prevent similar attacks and reduce their impact (Gregory, 2022). Finally, the chemical spill following a train derailment in East Palestine, Ohio in February 2023, made the potential devastation posed by an intentional cyber-attack on the transportation and/or chemical sector even more visible. According to the National Transportation Safety Board, a 38-train car derailment was followed by a fire which caused damage to an additional 12 cars (Hauser, 2023). The train was carrying chemicals and combustible materials containing a toxic flammable gas (Hauser, 2023). The derailment, led to evacuation orders in both Pennsylvania and Ohio on either side of the fires, placing thousands of residents at risk (Hauser, 2023). While the toxic chemicals were released from tankers and burned off, the risk faced by local residents included pollution to the air, soil, and water supply (Hauser, 2023). As the second largest chemical manufacturer in the world, unauthorized access to chemical facilities or distribution methods have the potential to devastate the physical and economic well-being of Texas.

Consistent operation of the energy sector ensures the health and welfare of Texans by ensuring steady energy is supplied via electricity, oil, and other natural gas resources, with 43 percent of America's oil refineries located along the Texas and Louisiana coasts. Primarily owned and run in the private sector, Texas' energy infrastructure supplies fuel to the transportation industry, and ensures power distribution to over 26 million customers via natural gas, wind, coal, nuclear, and solar resources (Wind Energy in Texas, n.d.). Ninety percent of the electric load in Texas is managed by the Electric Reliability Council of Texas (ERCOT) who ensures power distribution to over 26 million customers, connects more than 52,700 miles of transmission lines, and 1,100 generation units (About ERCOT, n.d.). Texas' independent and separate electrical grid is well-known and comprises one of three primary power grids in the United States. Texas' power grid relies on smart technologies that are mostly capable of identifying and preventing known threats (Cheri, Fofana, & Yang, 2021). While most commonly motivated to take advantage of electricity market interactions and electricity price fluctuations (Ahmadian, Malki, & Han, 2018), recent ransomware attacks aimed at Western targets, highlight just some of the challenges in securing the sectors cyber networks. In recent years, extreme weather events, such as the winter storm in February 2021, led to the widespread failure of electric generation facilities across the state. Extreme conditions led to blackouts affecting millions of residents, causing extensive property damage upwards of 80-130 billion dollars, and contributing to at least 210 deaths. These outages combined freezing weather conditions forced businesses to close, icy roads made driving impossible, people were unable to stay warm, they could not prepare food, and operate life-saving medical devices were in cases inoperable. And these were just the effects of a weather event. Consider the potential for harm in the event of a targeted cyber-attack.

As the demand on the state's power grid continues to grow, the threat posed by intentional cyber-actors becomes more significant as the energy sector is an increasingly popular target for hackers experiencing more than 40 industry attacks between 2017-2018 alone (Krauss, 2018). Energy companies are even more vulnerable due to the types of data they possess including consumer and business data as well as proprietary information about their holdings, trading strategies and exploration and production technologies (Krauss, 2018). One of the most infamous cyber-attacks against industrial control systems that threatened energy production critical infrastructure in the United States was a cyber campaign carried out by the cyber espionage group

Dragonfly in 2014 and from 2015-2017 (Chowdury & Gkioulos 2021). These hackers were interested in learning both how each energy facility operated as well as how to gain access to operational systems, the Dragonfly potentially obtained the ability to sabotage or gain control of electricity grids and nuclear facilities around the country (Threat Hunter Team, 2017). Their second campaign, Dragonfly 2.0 campaign, further utilized multiple techniques, including malware, to gain access to numerous computer systems and mount sabotage operations that could have disrupted energy supplies (Chowdury & Gkioulos, 2021). This type of intentional disruption to the energy critical infrastructure in Texas could have devastating consequences particularly as the state's population and demand for power continue to grow.

In the coming years, cyber threats to Texas' critical infrastructure will continue to increase. Industry leaders in critical infrastructure must work with government agencies to prepare for, defend against, and respond to cyber intrusions. Cyber-security, at a minimum, ensures that critical infrastructure providers are protected against the criminal or unauthorized use of electronic data. Cyber-security firms are commonly used by both public and private sector providers to ensure the safety and upkeep of their client's cyber networks, systems, connected devices, clouds, and databases through the provision of technology support, managed services, software tools, penetration testing, systems auditing, and vulnerability analysis. While this type of protection is imperative for the protection of critical infrastructure, consider the fallout from a cyber-attack on one of these firms. In 2020, the Texas-based cyber-security firm SolarWinds, was breached by the Russian Foreign Intelligence Service (RSV). The firm provides secure public sector IT management and monitoring services, including regular software updates. During a regular software update providing bug fixes and performance enhancements, hackers simultaneously exploited this vulnerability by taking the opportunity to gain access to, and install malicious software on, SolarWinds widely used network management system, Orion (Temple-Raston, 2021). This intrusion represents a massive cyber-attack against the United States that gave hackers access to thousands of client networks, comprised the cyber-security of roughly 100 companies, including Microsoft, Intel, and Cisco, and also gave them access to roughly a dozen government agencies, including the Treasury, Justice and Energy departments, the Pentagon, and the Cybersecurity and Infrastructure Security Agency (CISA) (Temple-Raston, 2021). The breadth and type of access they obtained was concerning on multiple fronts, including the possibility of hackers ability to

steal, alter, or destroy data, which could have had devastating consequences if targeted at critical infrastructures (Temple-Raston, 2021). While the impact of this attack was not nearly as bad as it could have been, this type of intrusion has the possibility of causing significant cyber-, and even physical-, damage to the Texas' critical infrastructure.

Way Forward

Moving forward, it is vital that government agencies, critical infrastructure providers, and cyber-security experts work together to identify cyber-threats, ensure the readiness of cyber systems to respond to these attacks, and develop solutions for implementation in the event of a cyber-attack. Cyber-attacks are often successful because of user lack of awareness or formal staff training (Chowdury & Gkioulos, 2021). Therefore, in order to respond to a cyber-attack, providers should understand the most prominent types of cyber-threats they are facing. The most common form of cyber-threat facing critical infrastructure are phishing attacks. Phishing occurs when a cyber-actor sends communication mimicking a trusted source to gain access to a cyber-network or system (Johnson, 2015). For critical infrastructure, these attacks may take the form of an email sent to a large group of employees attempting to gain access to a company's cyber network via one of their accounts. For example, hackers would send an email to every employee of a large airline asking them to authenticate their credentials to be able to download a software update with enhanced cybersecurity features. The email might appear to come from a corporate office but would actually contain malicious software in the download link that would allow hackers access to the airline's cyber networks. Related is spear phishing, a more targeted version of phishing, wherein cyber-attackers will research email recipients ahead of time to make their emails appear to be even more legitimate. For example, they might craft an email to a team of utility customer service representatives asking them to click a link to download a software update. The email would appear as though it came directly from their team lead or supervisor, as the from email address would contain this person's name, but it would actually be from a fake email account that is like an actual company email address, but with small differences that would make it difficult to notice if the email was not read carefully. Zero-day attacks are additional threats that occur when hackers identify and exploit weaknesses in a network, software, or hardware before a company has discovered and resolved the issue (Johnson, 2015). Denial-of-Service (DoS) attacks are also

prevalent occurring when a network, or device, is bombarded with traffic, overwhelming a system, and preventing it from functioning normally. They can cause systems to crash and prevent them from responding to legitimate requests from customers or employees. Malware/ransomware are among the biggest threats to critical infrastructure. Malware is malicious software that can spy on communications, steal information, damage, or destroy data, or encrypt files once in a cyber network. Ransomware is a type of malware that encrypts files on a corrupted network making it impossible for legitimate users to access these systems and bringing industrial operations to a halt. Once in a system, hackers will ask for a "ransom" to be paid in order to restore access, or decrypt files, so that legitimate use and business can resume. Malware and ransomware can enter a system in multiple ways, including external phishing attacks or internal intentional network intrusion, such as via a corrupted flash drive.

Since 2010, the federal Government Accountability Office (GAO) has called for improvements to cybersecurity around critical infrastructure. In 2017, the President's National Infrastructure Advisory Council likened the nation's cyber positioning to be equivalent to a pre9/11-level cyber moment, with a narrow and fleeting window of opportunity to coordinate resources effectively. And in early 2023, President Biden issued an executive order prioritizing the expansion of minimum-security requirements for critical infrastructures as well as improvements in collaboration between public and private sector entities to develop a more expedient and effective cyber incident response. The National Infrastructure Protection Plan (NIPP) further outlines the national vision for protecting critical infrastructure (Cybersecurity and Infrastructure Security Agency, 2019):

> A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened. This vision drives the basic approach to critical infrastructure security and resilience in the United States, to: Strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.

Identifying and responding to emerging and ongoing cyber threats requires that stakeholders across critical sectors communicate and collaborate to develop cyber response plans. Information sharing

within each sector is among the most important activities of an effective and efficient cyber response plan (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016). The ability to provide actionable threat information to owners and operators of these networks allows them to implement plans and take appropriate action in response to cyber-attacks. Housed in North Texas, Region 6 of the federal governments' CISA delivers services to support the security and resilience of critical infrastructure to owners and providers in conjunction with state, local, tribal, and territorial partners (Cybersecurity and Infrastructure Security Agency, 2019). Together, with well-trained cyber-security professionals, critical infrastructure providers should ensure they have an up to date cyber security response plan in place before an incident occurs. The plan should be among the first steps in generating a culture of cyber-security where every person knows their role and takes action. The plan should be approved by senior leadership and should clarify the roles and responsibilities for critical personnel and their tasks before, during, and after a confirmed or suspected cyber incident (Incident Response Plan (IRP) Basics, n.d.). The incident response plan, should, at a minimum, incorporate the following procedures (Incident Response Plan (IRP) Basics, n.d.):

1. Before a cybersecurity incident
    - Train all staff. Since many attacks are possible due to lack of training, missing protocols, or human error, equipping employees with the knowledge, tools, and awareness to be vigilant and responsive can go a long way toward ensuring network security. Ensuring all staff understands their role in ensuring the security of the organization, as well as how to report suspicious events are imperative to an effective plan.
    - Review cyber response plan with an attorney, CISA regional team 6, and local law enforcement. Collaboration among each of these ensures the most up to date and comprehensive plan is put into place.
    - Print the document and associated contact list and distribute to all personnel. This ensures everyone has access to the information in the event of an attack when digital communication will be shut down.

- Develop a plan and make sure everyone is aware of the role that they play, including who will need to be notified in the event of an attack. This could include board of directors, key investors, and critical partners.
- Review the plan quarterly and adjust in accordance with current threats.
- Prepare press responses in advance.
- Select an outside technical resource or firm that will investigate any breaches.
- Conduct attack simulation exercises to ensure that everyone knows their role and carries it out appropriately.

2. During a cybersecurity incident
    - Assign an Incident Manager who will be responsible for leading the response managing how communication flows, updating stakeholders, and delegating tasks. This person should not be responsible for performing any technical duties.
    - Assign a Tech Manager who will serve as the subject matter expert that brings together internal and external experts.
    - Assign a Communications Manager to interact with reporters, post updates on social media, and interact, as needed, with external stakeholders.
3. After a cybersecurity incident
    - Hold a formal retrospective meeting to report out the known incident timeline and ask for additions and edits. Security breaches are often the result of multiple person's actions, so make sure these reports are blameless to ensure that all participants feel comfortable speaking freely about the incident.
    - Update policies and procedures based on the meeting.
    - Communicate findings to staff. This contributes to a culture of security and builds trust among staff showing that cyber-security threats are taken seriously. Critical infrastructure providers should further ensure the following practices (5 ways to prevent cyber-attacks against critical infrastructure, n.d.):

    1. Be vigilant and read all emails with a critical eye looking for inconsistencies, grammatical errors, looking for known senders etc. to avoid exposing cybersystems to cyber-threats.

2. Ensure all networks, systems, and software are up to date and that security patches are applied regularly to avoid vulnerabilities that might leave an opening for a hacker to enter the system.
3. Require strong passwords before access to any critical systems.
4. Utilize multi-factor authentication to ensure only legitimate access to critical cyber networks and systems.
5. Audit devices, assets, and other network components regularly

Finally, utilities and industrial partners should share best practices for network security and encourage transparency by reporting known cyber-attacks to the appropriate government agency, software providers, other critical infrastructure providers, and the network cybersecurity team for the most timely and efficient response possible. The development and adoption of Artificial Intelligence (AI)-enabled cyber-defense techniques are also needed to protect smart enabled infrastructure to respond to the constantly evolving nature of contemporary cyber-attacks (Koroniotiset et al., 2020).

Texas remains particularly vulnerable to cyber threats as a desirable location to live, work, and conduct business. We have the 9th largest economy in the world, are home to headquarters of more than 50 fortune 500 companies and are the leading destination for companies relocating from other states. For 20 years in a row, Texas has been the number 1 U.S. exporter, with exports totaling approximately $375 billion in 2021. We are the largest energy-producing state in the nation, and are home to 26 commercial airports, 19 seaports, 22 interstate highways, and 58 freight railroads. Our cyber vulnerabilities are plentiful with many attractive targets for cyber criminals and organizations around the world. It is imperative industry leaders are able to recognize and identify their cyber risks to develop prevention strategies and respond to cyber-attacks more quickly and effectively. Disruptions to critical infrastructures could lead to theft of intellectual property; supply chain disruption; electricity disruption; loss of operations capacity; or chemical theft, diversion, or release. Texas' industrial vulnerability to cyber-attacks through phishing, ransomware, and malware pose significant threats to the security of our critical infrastructures and daily life. Both public and private sector cybersecurity professionals must remain cognizant of their responsibility to secure the states most important cyber networks.

References

5 Ways to Prevent Cyberattacks on Critical Infrastructure. (n.d.). *Unearth*. https://www.unearthlabs.com/blogs/cybersecurity-critical-infrastructure

About ERCOT. (n.d.). *ERCOT*. https://www.ercot.com/about

Ahmadian, S., Malki, H., & Han, Z. (2018, November). Cyber attacks on smart energy grids using generative adverserial networks. In *2018 IEEE global conference on signal and information processing (GlobalSIP)* (pp. 942-946). IEEE.

Chehri, A., Fofana, I., & Yang, X. (2021). Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability*, 13(6), 3196.

Chemical Sector. (n.d.). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructuresectors/chemical-sector

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Cimpanu, C. (2018, November 16). Trump signs bill that creates the Cybersecurity and Infrastructure Security Agency. *ZDNET/tech*. https://www.zdnet.com/article/trump-signs-billthat-creates-the-cybersecurity-and-infrastructure-security-agency/

Cormier, A., & Ng, C. (2020). Integrating cybersecurity in hazard and risk analyses. *Journal of Loss Prevention in the Process Industries*, 64, 104044. https://doi.org/10.1016/j.jlp.2020.104044

Cost of a Data Breach Report 2023. (n.d.). *IBM*. https://www.ibm.com/reports/databreach?utm_medium=OSocial&utm_source=Blog&utm_content=SSSWW&utm_id=SecurityIntelligence-Blog-CTA-Button&_ga=2.135027761.1494275948.1692636260-1782696331.1692636260&_g

Creation of the Department of Homeland Security. (n.d.). *U.S. Department of Homeland Security*. https://www.dhs.gov/creation-department-homeland-security

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Cybersecurity Division. (n.d.). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/about/divisions-offices/cybersecurity-division

Cybersecurity and Infrastructure Security Agency. (2019, November). A Guide to Critical Infrastructure Security and Resilience. *CISA*. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-SecurityResilience-110819-508v2.pdf

Ellis, T., Locasto, M., & Balenson, D. (2020). Cyber State Requirements for Design and Validation of Trust in the Critical Transportation Infrastructure. In *Critical Infrastructure Protection XIV: 14th IFIP WG 11.10 International Conference, ICCIP 2020, Arlington, VA, USA, March 16–17, 2020, Revised Selected Papers* 14 (pp. 69-83), 10.1007/978- 3-030-628406_4. hal-03794631f

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 35(2), 486-505. https://doi.org/10.1057/s41284-021-00286-2

Gregory, J. (2022, September 28). Cost of a Data Breach: Infrastructure. *Security Intelligence*. https://securityintelligence.com/articles/cost-data-breach-infrastructure/

Hauser, C. (2023, June 23). After the Ohio Train Derailment: Evacuations, Toxic Chemicals and Water Worries. *The New York Times*. https://www.nytimes.com/article/ohio-trainderailment.html

Incident Response Plan (IRP) Basics. (n.d.). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Introduction to the Chemical Sector Risk Management Agency. (n.d.). Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/Chemical%2520SRMA%2520Fact%2520Sheet_508.pdf

Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International journal of production research*, 58(10), 2904-2915.

Johnson, T. A. (Ed.). (2015). *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare.* CRC Press.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. *NIST special publication*, 800(150).

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. *IEEE Access*, 8, 209802209834. doi: 10.1109/ACCESS.2020.3036728

Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022). What changed in the cyber-security after COVID-19?. *Computers & Security*, 120, 102821. https://doi.org/10.1016/j.cose.2022.102821

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, 105, 102248. https://doi.org/10.48550/arXiv.2006.11929

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future internet*, 12(9), 157. https://doi.org/10.3390/fi12090157

Lehto, M. (2020). Cyber Security in Aviation, Maritime and Automotive. In: Diez, P., Neittaanmäki, P., Periaux, J., Tuovinen, T., Pons-Prats, J. (eds) Computation and Big Data for Transport. Computational Methods in Applied Sciences, vol 54: 19-32. Springer, Cham. https://doi.org/10.1007/978-3-030-37752-6_2

Lim, H. S. M., & Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*, 11(5), 1062. doi:10.3390/en11051062

McPherson, K., Donald, J., Wright, B. (2018, May). Transportation Infrastructure. *COMPTROLLER.TEXAS.GOV*. https://comptroller.texas.gov/economy/fiscalnotes/2018/may/transportation.php

Montague, Z. (2023). Russian Ransomware Group Breached Federal Agencies in Cyberattack. *The New York Times*. https://www.nytimes.com/2023/06/15/us/politics/russian-ransomwarecyberattack-clop-moveit.html

Ponemon Institute. (2019). Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?. *Siemens*. https://assets.new.siemens.com/siemens/assets/api/uuid:c723efb9-847f-4a33-9afa8a097d81ae19/version:1633555091/siemens-cybersecurity.pdf

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iotenabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, 20(4), 3453-3495.

Tal, J. (2018, September 20). America's Critical Infrastructure: Threats, Vulnerabilities and Solutions. SecurityInfoWatch.com. https://www.securityinfowatch.com/access-identity/accesscontrol/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions

Temple-Raston, D. (2021, April 16). A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. *NPR*. https://www.npr.org/2021/04/16/985439655/a-worst-nightmarecyberattack-the-untold-story-of-the-solarwinds-hack

Texas Comptroller. (n.d.). *Chemical Manufacturing Supply Chain*. COMPTROLLER.TEXAS.GOV. https://comptroller.texas.gov/economy/economic-data/supplychain/2021/chem.php

Threat Hunter Team. (2017, October 20). Dragonfly: Western energy sector targeted by sophisticated attack group. *Symantec*. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Transportation Systems Sector. (n.d.). *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructuresectors/transportation-systems-sector

Transportation Systems Sector-Specific Plan. (2015). Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015508.pdf

Wind Energy in Texas. (n.d.). Office of Energy Efficiency & Renewable Energy. https://windexchange.energy.gov/states/tx

Yeh, E., Choi, J., Prelcic, N. G., Bhat, C. R., & Heath, R. W. (2018). *Cybersecurity challenges and pathways in the context of connected vehicle systems* (No. D-STOP/2017/134). University of Texas at Austin. Data-Supported Transportation Operations & Planning Center (D-STOP).

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

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.

Institute for Homeland Security
Sam Houston State University

Nodeland, B. (2023) Ensuring the Cybersecurity of Texas' Critical Infrastructures. (Report No. IHS/CR-2023-1023). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/4ZVRU