INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

RANSOMWARE: A CONTEMPORARY SECURITY THREAT

Institute for Homeland Security

Sam Houston State University

Michael S. Vaughn

In the contemporary digital world, the destructive force of cyberattacks costs millions of dollars, adversely impacting economies, critical infrastructure, and most industries (Brunner, 2020). A type of cyberattack, ransomware, is particularly destructive. Ransomware is a type of "malware that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom" (Farringer, 2017, p. 953). In the United States in 2020, the FBI's Internet Crime Complaint Center (IC3) reported "2,474 ransomware complaints" with losses exceeding $29.1 million (Berris & Gaffney, 2021, p. 2). Most experts agree that ransomware attacks are grossly underreported since these "incidents are often addressed by the victim directly and are never reported to the public or law enforcement" (Berris & Gaffney, 2021, p. 2).

The Texas Cybercrime Act (TCA) amended the Breach of Computer Security Act (BCSA) (Tex. Penal Code § 33.02, et seq., 2017), making "ransomware, malware, and direct denial of service attacks" specifically illegal in Texas (Tuma, 2018, p. 28). The TCA also requires governmental entities "to make cybersecurity a top priority" (Tuma, 2018, pp. 28-29). TCA requirements will empower state agencies to better assess risks and vulnerabilities, enabling them to defend more appropriately against cyberattacks (Rogers, 2018). Cybersecurity mandates for state agencies under the TCA include "risk assessments, cyber risk management, planning, vulnerability and penetration testing, and incident response planning" (Tuma, 2018, p. 28).

Ransomware specifically poses direct threats to the transportation, health care, energy, and chemical sectors of society. This paper addresses ransomware from a legal perspective, identifying federal laws that have been enacted to combat ransomware. The paper also assesses how ransomware has impacted the transportation, health care, energy, and chemical sectors in

Texas. The paper concludes by recommending that the State of Texas create an agency to report cyber threats in general and ransomware specifically.

Ransomware Legislation

The frequency and mounting financial toll that ransomware has posed to critical infrastructure has received increased attention. The May 2021 ransomware attack on the Colonial Pipeline, for example, aroused the interest of the public and politicians due to shortages of gasoline and price hikes on the East Coast (McMillan et al., 2021). Colonial Pipeline reportedly paid the Russian ransomware attackers $4.4 million, but the U.S. government later recovered some of the ransom (Austin, 2021). At the federal level, Congress enacted in 2022 a ransomware reporting law. Up until recently, most hacking and those involving ransomware were prosecuted under the Computer Fraud and Abuse Act (CFAA) of 1986 as amended, which has both criminal and civil provisions. The CFAA penalizes unauthorized access, use, and the imbedding of malware, such as ransomware. CFAA also prohibits intentionally using a computer and passwords with the intent to damage, defraud or extort information or expose confidential information (McNicholas & Angle, 2021).

On March 15, 2022 Congress passed the Consolidated Appropriations Act of 2022 (CAA). What has become a frequent practice of Congress, the CAA was an omnibus bill that funded practically every branch of the federal government, including the Departments of Agriculture, Commerce, Labor, Education, Defense, Veterans Affairs, Energy, Interior, Health and Human Services, Homeland Security, Environment, State, Transportation, Housing and Urban Development, and the General Services Administration. When President Biden signed the CAA, part of that law was the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). With respect to ransomware, the CIRCIA amended the Section 103 of the Homeland

Security Act of 2002 by providing a "cyber incident reporting" division, entitled the Cybersecurity and Infrastructure Security Agency (CISA). CIRCIA also amended Section 2240 of the of the Homeland Security Act of 2002 by including definitions of a "ransomware attack":

> (A) means an incident includes use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromises the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and
>
> (B) does not include any such event where the demand for payment is
>
> a. not genuine; or
>
> b. made in good faith by an entity in response to a specific request by the owner or operator of the information system.

CIRCIA also defined a "ransom payment":

> The term ransom payment means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

CIRCIA was primarily enacted to enhance and augment cyber incident reporting and information sharing among government agencies and companies outside of government labeled as critical infrastructure. Housed within the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA) is the government entity that records ransomware attacks reported by federal agencies and private companies. The Director of the CISA, along

with the other intelligence entities in the government, assists the President to establish the National Cybersecurity Posture.

Pursuant to the Cybersecurity Information Sharing Act of 2015, the CISA must receive, analyze, coordinate, and share cyber incidents, including ransomware. These activities involve prioritizing ransomware attacks, classifying incidents as part of a group or a lone wolf, providing a detailed examination of the nature of the attack, and categorizing and distributing measures to avoid, counteract, and ameliorate future attacks of comparable magnitude. Every 60 days, the CISA Director must also brief high ranking governmental officials about the "national cyber threat landscape," including ransomware attacks on any federal or intelligence agencies and any critical infrastructure. The briefing should provide action steps recommended to reduce threats and the ability of actors to appropriately respond to or prevent ransomware attacks.

CIRCIA's main change in the legal landscape is its required reporting mandates of certain cyber incidents and ransomware attacks on federal agencies and private sector entities considered critical infrastructure. The Director of CIRCIA is charged with creating guidelines that specify what entities are "critical infrastructure." While CIRCIA does not define the companies and businesses that are considered critical infrastructure, it does points to guideposts which were established in the Presidential Policy Directive (PPD) 21 from 2013. The PPD 21 "deems the following sectors as critical infrastructure: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base, emergency services, energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems" (Beringer et al., 2022, p. 1). Under CIRCIA, federal agencies and critical infrastructure entities must report cyber incidents to CISA within 72-hours of their

discovery. Moreover, these agencies and businesses must report to CISA within 24-hours if a ransom is paid in a ransomware attack. Any company that pays a ransom in a ransomware attack must report it to the CISA, even if they are not critical infrastructure as determined by the guidelines promogulated by the CISA Director.

Under CIRCIA, companies must report cyber incidents that are "substantial," meeting the "definition and criteria" to be established by the Director of CISA. A substantial disruption includes ransomware attacks that deny service to work product, exploit "information systems or networks; or an operational technology system or process; or unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise." Those who report ransomware to CISA are "exempt from disclosure" under the Freedom of Information Act (FOIA), as well as state or local laws pertaining to open government, open meetings, open records, or sunshine laws that require disclosure of records.

Ransomware as a Contemporary Threat to Transportation, Healthcare, Energy, and Chemical Sectors in Texas

Energy Sector. The Texas energy sector produces over $172 billion per year. Corporate headquarters for ExxonMobil, Occidental Petroleum, and BP are located in Texas. The energy sector in Texas employees over 292,000 people and has over 55,600 clean energy jobs. Moreover, Texas leads the nation in crude oil production with a refining capacity of over 5.1 million barrels of oil per day, which accounts for 28% of the nation's refining capacity (Texas Economic Development Corporation, 2022). Indeed, revenue from the oil, gas, refining, and pipeline industry generates over $43 million per day in Texas (Takahashi, 2022).

The wealth that Texas generates from its energy sector makes it a prime target for hackers determined to install malware on industry servers and computers. The Colonial Pipeline ransomware attack that caused significant shortages of gasoline on the East Coast should give cybersecurity officials pause within Texas' energy sector (Eaton et al., 2021). Texas infrastructure, for example, is not immune to cyber intruders. While not involving the energy sector, the ransomware attack of 23 small Texas towns during the middle of August in 2019 sent shockwaves around the state (Fazzini, 2019). Moreover, since starting the War in Ukraine, Russian hackers have attempted to infiltrate the energy sector of Texas, looking for weak spots in infrastructure to interrupt operations and/or steal critical information and data. It was Russian-based cyber criminals who unleashed the ransomware attack on the Colonial Pipeline, and there are concerns of a similar attack on the energy industry in Texas or on the fragile Texas power grid (Ferman, 2022). CISA recently released a memorandum, saying that "evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks," including efforts to interrupt Texas' power grid (Mooney, 2022). Russian hackers are also exploring ways to disrupt the Port of Corpus Christi, which has become one of the nation's largest natural gas exporting hubs. Russia seeks to disrupt natural gas exports from the U.S. since European countries are attempting to reduce reliance on Russian oil and gas.

Chemical Sector. Other than China, the United States manufactures the most chemicals in the world, and Texas leads the country in the production of "plastics, packaging, fertilizers, pesticides, synthetic fibers, cleaners, lubricants, and paint" (Hegar, 2021). According to the American Chemical Counsel, Texas produced $117.5 billion of chemicals in 2021. During the Winter storm in February 2021, Texas' power grid collapsed, and the nation's chemical industry was disrupted for months. While there has not been a big ransomware attack in the chemical

sector that is widely known, similar to the energy industry, the chemical sector also faces cybersecurity threats. Indeed, industry leaders have opined that the petrochemical industry's supply chain is susceptible to cyberattacks (Hegar, 2021). The same factors that make the energy sector vulnerable to cyber criminals also expose the chemical industry to potential ransomware attacks. The sheer amount of data generated within chemical manufacturing make the sector "inherently difficult to manage and secure" (Hegar, 2021).

Healthcare Sector. Texas has one of the largest medical infrastructures in the world. According to the University of Texas at Arlington (2019), 32% of the largest employers in Texas have employees working in some aspect of health care. In 2016, health care contributed around $105 billion to the GDP of Texas (Hegar, 2018). With the escalation of medical technology and the move to electronic medical records, however, health care systems are extremely vulnerable to cyberattacks. The Clinic of North Texas, for example, reported an unauthorized November 2021 infiltration of a network server, where 244,200 patients' private health information was stolen (McGee, 2022). These patients are at increased risk of identity theft and fraudulent schemes to "buy back" their medical information.

In another ransomware attack, in September 2022 OakBend Medical Center in Richmond, Texas reported that after a ransomware attack it "took all systems offline, placed them in lockdown mode," and called the FBI and other law enforcement officials. Saying that "at no time was patient safety ever in jeopardy," a week after the ransomware attack the hospital reported that it was in the process of "rebuilding and that the phones and email were still impacted" (Diaz, 2022). Moreover, several weeks after the ransomware attack, OakBend reported that "despite taking reasonable precautions, the unauthorized" attack resulted in the theft of "sensitive patient and employee data" (McKeon, 2022). Additionally, after the

ransomware attack, the hospital confirmed that it has "implemented multi-factor authentication and installed a new software system to monitor for future threats" (McKeon, 2022).

Transportation Sector. Transportation is big business in Texas; the 2022-2023 FY budget for the Texas Department of Transportation (TX DOT) is over $30 billion (TX DOT, 2022). Even with that budget, TX DOT is not immune from cyberattacks. In May of 2020, TX DOT was hacked and subject to a ransomware attack. It was the second ransomware attack of a State of Texas governmental agency during the same week. A few days before TX DOT was hacked, the Texas Office of Court Administration, the record keeping agency for the Texas appellate court system, reported a ransomware attack. Upon noticing the ransomware attack, TX DOT staff "immediately isolated the affected parts of the network and shut down further unauthorized access." The Executive Director of the TX DOT said that his "staff was working to ensure critical operations continue during this interruption" (CBS DFW, 2020).

> Antivirus company PC Matic released a statement on the ransomware against the courts agency, saying in part: 'Cyber criminals strike Texas again – the Texas Office of Court Administration is the latest victim in a string of attacks that have targeted the United States admist the COVID-19 pandemic, and it is far past time that state and local leaders get serious about solving this problem once and for all...' (CBS DFW)

The transportation sector also includes trains, automobiles, and airplanes. With respect to vehicles, there is no known ransomware attacks to date; however, hackers have infiltrated car dealers' software, vehicle GPS systems, and car alarms. There is a real possibility that a ransomware attack could disable a vehicle, requiring the driver to pay a ransom in order to start the engine (Kamping-Carder & Hand, 2020). With respect to trains, they are computer operated and many possess internal wi-fi networks. Technology which accelerates and decelerates trains

to avoid human error could be hacked and cause derailments and/or train collisions. As for airplanes, they operate with an abundance of technological systems, "and an airplane's flight-control system isn't the only target: Systems managing ground-crew personnel, air-traffic control, airport kiosks, aircraft catering, baggage claim, and plane-to-ground communication could all be attacked—all of which could prevent flights from taking off" (Kamping-Carder & Hand, 2020, pp. R4-R5).

Conclusion

While ransomware is a crime in Texas under the Texas Cybercrime Act, Texas needs a reporting agency much like that recently created by the federal government. To protect the transportation, energy, chemical, and healthcare sectors, Texas needs to develop mandatory cybersecurity standards for these critical infrastructure entities. Texas also needs a repository where ransomware attacks are to be reported and a state agency that elevates ransomware attackers to the category of serious offenders. Indeed, the state should be surveilling the internet and dark web activities of suspected ransomware attackers. Such a state agency would also prepare a biennial report for each legislative session, reporting on recent developments and countermeasures with respect to ransomware.

References

Austin, P.L. (August 2-August 9, 2021). How one company refused to let cyber attackers win. *Time*, p. 16.

Beringer, A., Southwell, A.H., Bergsieker, R.T., & Tapia, S.S. (March 22, 2022). *President Biden signs into law the Cyber Incident Reporting for Critical Infrastructure Act, expanding cyber reporting obligations for a wide range of public and private entities*. Gibson, Dunn, & Crutcher LLP. https://www.gibsondunn.com/wp-

content/uploads/2022/03/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities.pdf

Berris, P.G., & Gaffney, J.M. (October 5, 2021). Ransomware and federal law: Cybercrime and cybersecurity. *Congressional Research Service*. https://crsreports.congress.gov/product/pdf/R/R46932

Brunner, M. (2020). Challenges and opportunities in state and local cybercrime enforcement. *Journal of National Security Law & Policy*, *10*(3), 563-582.

CBS DFW. (May 17, 2020). TX government agencies hacked for 2nd time in week. *CBS DFW*. https://www.cbsnews.com/dfw/news/texas-government-agencies-hacked-2nd-time-in-week/

Computer Fraud and Abuse Act (CFAA) – 1986. 18 U.S.C. § 1030.

Consolidated Appropriations Act (CAA) – 2022. PL 117-103.

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) – 2022, HR 2471.

Cybersecurity Information Sharing Act (CYSA) – 2015. 6 U.S.C. § 1591.

Diaz, N. (September 12, 2022). Texas hospital hit by ransomware attack. *Becker's Health IT*. https://www.beckershospitalreview.com/cybersecurity/texas-hospital-hit-by-ransomware-attack.html

Eaton, C., Rundle, J., & Uberti, D. (May 10, 2021). Pipeline's shutdown exposes cyber threat to power sector. *The Wall Street Journal*, pp. 1A-2A.

Farringer, D.R. (2017). Send us the bitcoin or patients will die: Addressing the risks of ransomware attacks on hospitals. *Seattle University Law Review, 40*(3), 937-986.

Fazzini, K. (August 22, 2019). Texas ransomware attacks show big gaps in cyber defense – expect more like them. *CNBC.* https://www.cnbc.com/2019/08/22/texas-ransomware-attacks-tell-the-us-cybersecurity-story.html

Ferman, M. (March 31, 2022). Texas power grid, energy sectors facing elevated Russian cyber threats during war with Ukraine. *The Texas Tribune*. https://www.texastribune.org/2022/03/31/texas-energy-grid-russia-cyberattack-hackers/

Hegar, G. (2018). Education and health services overview: Women in the workforce. *Texas Comptroller of Public Accounts*. https://comptroller.texas.gov/economy/economic-data/women/health-education-overview.php#:~:text=Quick%20Facts,all%20jobs%20in%20the%20state

Hegar, G. (2021). Supply chains: Chemical manufacturing supply chain. *Texas Comptroller of Public Accounts*. https://comptroller.texas.gov/economy/economic-data/supply-chain/2021/chem.php

Kamping-Carder, L., & Hand, K. (October 9, 2020). Hacking's next targets. *The Wall Street Journal*, pp. R4-R-5.

McGee, M.K. (April 8, 2022). Big hacks: 5 health data breaches affect 1.2 million. *Gov Info Security*. https://www.govinfosecurity.com/big-hacks-5-health-data-breaches-affect-12-million-a-18873

McKeon, J. (September 19, 2022). OakBend medical center confirms data theft following ransomware attack. *Health IT Security*. https://healthitsecurity.com/news/texas-hospital-rebuilding-communication-systems-after-ransomware-attack

McMillan, R., Volz, D., & Hobbs, T.D. (May 12, 2021). As ransomware attacks rise, consequences get more severe. *The Wall Street Journal*, pp. A1, A5.

McNicholas, E., & Angle, K. (2021). Cybersecurity laws and regulation USA. In N. Parker (Ed.), *Cybersecurity 2022*. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa

Mooney, M. (May 6, 2022). Why it's so hard to protect the Texas power grid. *Axios Dallas*. https://www.axios.com/local/dallas/2022/05/06/texas-power-grid-cybersecurity-challenges

Rogers, E. (2018). Leadership role: New laws are putting Texas at the forefront in addressing cybersecurity as a matter of public policy. *Texas Bar Journal*, *81*(10), 686-688.

Takahashi, P. (January 11, 2022). Texas oil and gas revenue increased by nearly $2B in 2021. *Houston Chronicle*. https://www.houstonchronicle.com/business/energy/article/Texas-oil-and-gas-industry-paid-15-8B-in-taxes-16767552.php

Texas Department of Transportation (TX DOT). (2022). Texas transportation funding: Fiscal years 2022-2023. *TX DOT*. https://ftp.txdot.gov/pub/txdot-info/fin/funding-brochure-2022.pdf

Texas Economic Development Corporation. (2022). *Energy sector in Texas*. https://businessintexas.com/business-sectors/energy/

Tuma, S.E. (2018). Cybersecurity and data privacy law. *Texas Bar Journal*, *81*(1), 27-28.

University of Texas at Arlington. (March 20, 2019). *Health care is big business in Texas*. https://academicpartnerships.uta.edu/articles/mba/healthcare-big-business-in-texas.aspx#:~:text=Healthcare%20Revenue%20in%20Texas&text=In%20the%20Dallas-Ft.,economic%20sectors%20in%20the%20region

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

Vaughn, M. S. (2022). **Ransomware: A Contemporary Security Threat**. (Report No. IHS/CR-2022-2045). The Sam Houston State University Institute for Homeland Security. https://ihsonline.org/Research/Technical-Papers/Ransomware-A-Contemporary-Security-Threat