Final Project

University of San Diego Cyber Threat Intelligence Plan Proposal

Daniel Cordeiro Marques

University of San Diego

CSOL-580-02-SP22 - Cyber Intelligence

Professor Todd Raines

February 27, 2022

Table Of Contents

Executive Summary

Cyberattacks continue to increase, and the University of San Diego (USD) may find it difficult to defend against all existing adversaries. Cyber Threat Intelligence (CTI) allows organizations to acquire intelligence from different sources to understand how adversaries operate and focus efforts on controls that efficiently defend against relevant threats. This CTI plan enumerates threats against USD and outlines controls that effectively mitigate risks associated with the University's operations.

As an educational institution that handles personally identified information from thousands of students and faculty, USD is a target for ransomware groups motivated by financial gain. Once they gain access to the target's network, these groups encrypt and steal sensitive data from the victim to profit from extortion. This plan also highlights lessons learned from past incidents associated with similar threats to draw recommendations to improve USD's cyber security posture.

To mitigate the risks associated with ransomware groups, this plan proposes seven initiatives that should be performed in the next three to eighteen months, focused on preventing threats in the early stages of the attack, detecting their activities during the event, and minimizing the impact upon successful compromise. The benefits of these initiatives outweigh the investment mainly by reducing the cost of recovering from an incident. For example, the recommended CTI solution could pay for itself in the second year of implementation and offer a significant return in three years (over 100% of return on investment).

Cyber Threats To University of San Diego

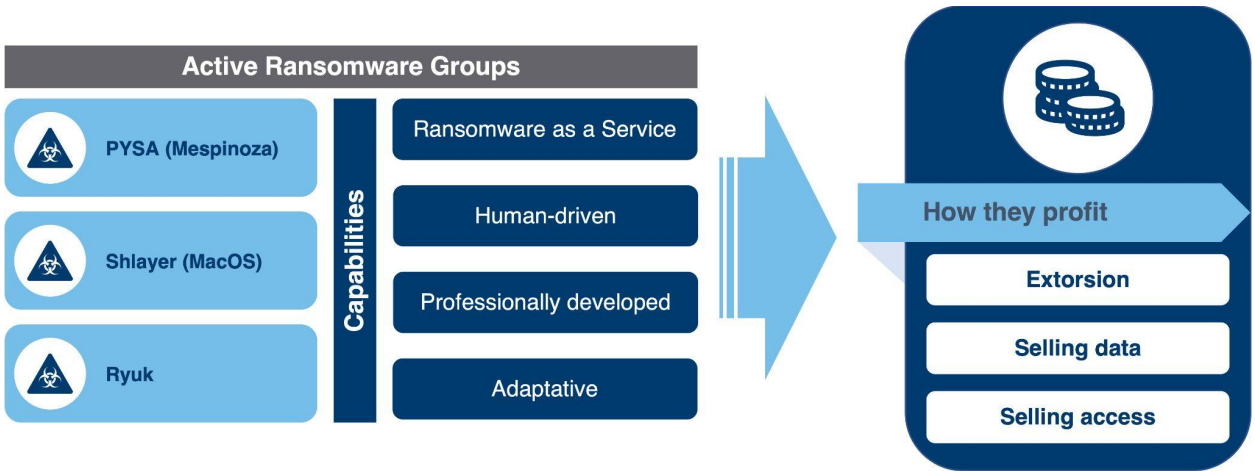
There are many ransomware attacks targeting education institutions, including higher education organizations (CISA et al., 2020; FBI, 2021). Organizations such as USD are prime targets for threat actors, as they store a high volume of student personally identifiable information (including social security numbers and payment information), proprietary research, and an IT infrastructure that may lack investments in security. In February 2020, the Gadsden Independent School District in Las Cruces, NM had to shut down its 24 schools to recover from a threat actor (Foresman, 2020). Months later, in Texas, Sheldon Independent School District "paid nearly $207,000 in ransom after hackers locked out officials from critical software systems" (Willey, 2020).

Threat Actors And Motivation

Active threat actors targeting educational institutions include PYSA (Mespinoza), Shlayer, and Ryuk (figure 1). These groups are motivated primarily by financial gain through encryption and theft of sensitive data to extort the victim, threatening to release the information publicly if the ransom is not paid (Bracken, 2021). Alternatively, they might sell access to the compromised hosts to launch attacks against other organizations as an additional revenue stream.

Figure 1.

Cyber Threats To USD.

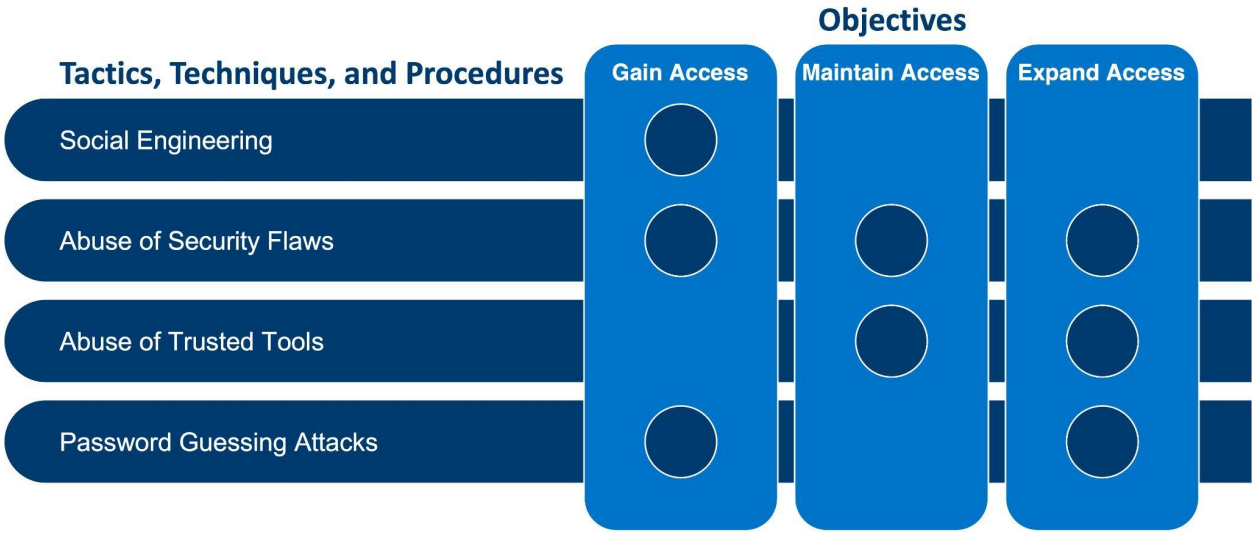


Capabilities And Attack Methods

These threat actors show signs of sophistication and organization. PYSA operates in a ransomware-as-a-service (RaaS) model through human-driven attacks (Milenkoski, 2021), targeting organizations that are more likely to pay the ransom. Lindblom (2021) highlights Shlayer's ability to quickly adapt, from using previously undisclosed vulnerabilities to using social engineering and compromised websites to deploy ransomware. The malicious software's dual-purpose indicates the groups' advanced capabilities: it encrypts and steals sensitive information using a combination of custom algorithms and serves as remote control of compromised systems. Figure 2 illustrates the groups' primary attack methods.

Figure 2.

Typical Attack Methods Utilized By Cyber Threats To USD.



Despite their efficiency, USD can still minimize the risk associated with these threat actors. Applying basic cyber security controls such as multifactor authentication and network segmentation will effectively reduce the risk of successful attacks.

Case Study: Outcomes of Cyber Security Incidents By Similar Threat Actors

The study of cyber security incidents can shed light on understanding the impact of similar threats to USD and prioritizing countermeasures to reduce the risk of a potential breach.

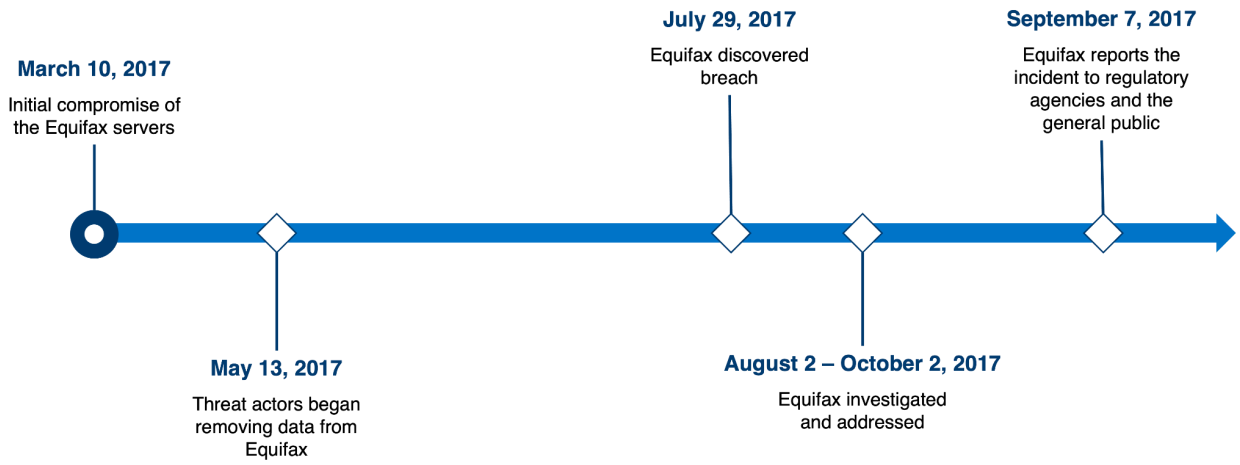
The 2017 Equifax Data Breach And Theft Of Data

On February 10, 2020, the United States Department of Justice announced charges against four alleged military-sponsored Chinese nationals (*Chinese Hackers Charged in Equifax Breach*, 2020). Potentially, the threat actors' objective was to collect data and "feed China's development of artificial intelligence tools as well as the creation of intelligence-targeting packages" (Barret, 2020).

The threat actors began by probing the Equifax Internet-facing network for systems running vulnerable software. Once they identified a vulnerability on Equifax's "Dispute Portal," the actors obtained a foothold in the internal network and gained access to a database with unencrypted PII, usernames, and passwords. Reusing these credentials, the threat actors expanded their access to compromise additional databases and slowly retrieved data from the environment through 76 days (GAO, 2018). Figure 3 illustrates the timeline of events.

Figure 3.

Timeline for the 2017 Equifax Data Breach (GAO, 2018).



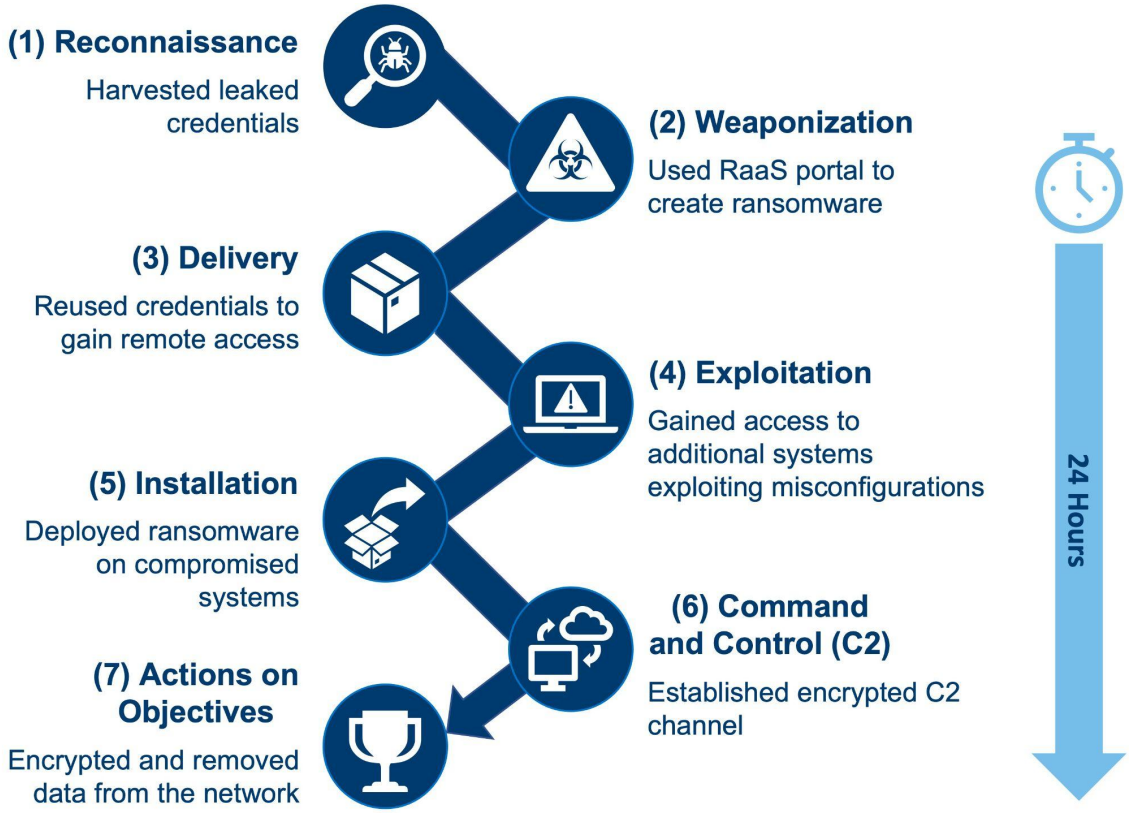
The 2021 Colonial Pipeline Ransomware Attack

In May 2021, Colonial Pipeline took the spotlight of major news outlets worldwide. A ransomware attack forced the shutdown of their pipelines, causing a panic buy that resulted in a temporary shortage of fuel in parts of the U. S. (Romo, 2021). The FBI attributed the attack to the DarkSide group (FBI National Press Office, 2021), a prolific threat actor that built a business model based on ransomware distribution. Financial gain is DarkSide's only motivation; the group claims they are not associated with political causes or governments (CrowdStrike Threat Intel Team, 2021).

DarkSide provides an example of how ransomware groups could gain access to USD's network and impact the University's operations. The analysis of the DarkSide's Cyber Kill Chain (figure 4) during this incident illustrates the group's sophisticated operations and highlights the utilization of human-driven activities during the attack. In approximately 24 hours, the group moved from the initial access to Colonial's enterprise network to successfully compromising servers and data.

Figure 4.

Colonial Pipeline Ransomware Attack Cyber Kill Chain.



Lessons Learned From Previous Breaches

Equifax and Colonial had opportunities to prevent and detect malicious activities in the early stages of the attack. Still, they failed to do so due to the lack of robust cyber security

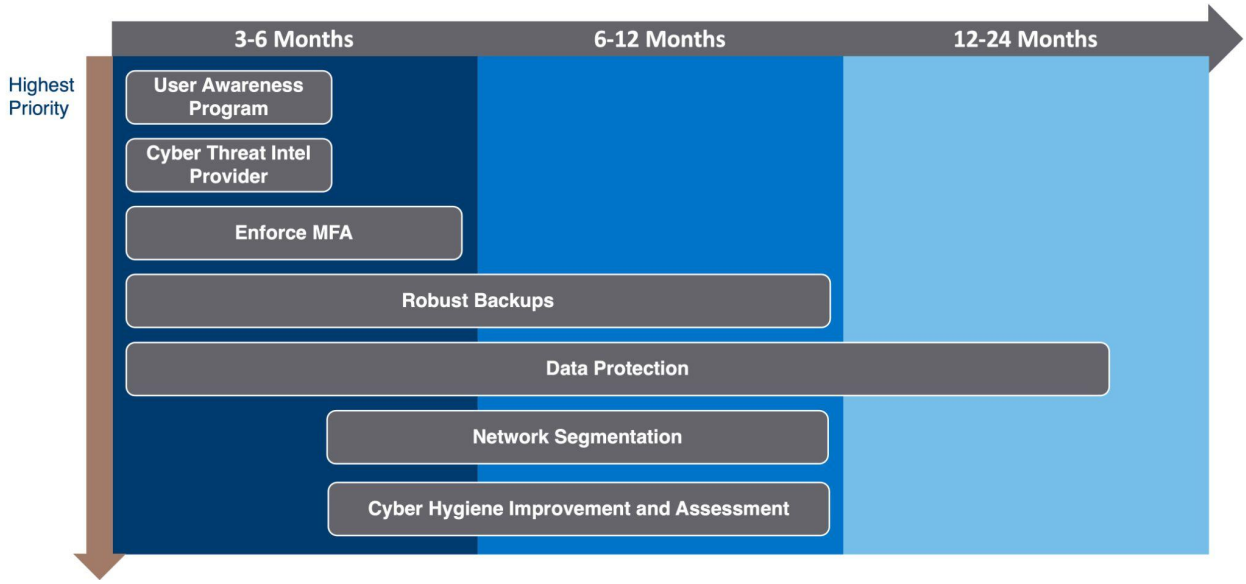
processes. Notably, they could not enforce an appropriate network segmentation, maintain a vulnerability and patch management process, and establish network and endpoint protection capabilities.

Risk Reduction Plan

This risk reduction plan focuses on addressing the threats described in this report through three perspectives: preventing threats in the early stages of the attack, detecting their activities during the event, and minimizing the impact upon successful compromise. Figure 5 outlines a roadmap to implement the recommended actions.

Figure 5.

Implementation Roadmap.



Establish A User Awareness Program

The *Verizon 2021 Data Breach Investigations Report* (2021) indicates that phishing attacks are the most common attack during a breach, which threat actors generally utilize to gain initial access to the target's network. USD should train users to identify and respond to social engineering attacks coming from email or direct interaction. The University should develop and

deploy employee awareness campaigns, formal training, and quarterly simulation exercises in the next three months.

Invest On A Cyber Threat Intelligence Provider To Improve Detection Capabilities

With continuously evolving threats, successfully understanding their tactics, techniques, and procedures are essential to secure organizations proactively. Therefore, threat intelligence products should offer actionable reports based on credible sources and easily integrate with threat detection tools to enhance the organization's security monitoring capabilities.

CrowdStrike Falcon Complete is the recommended tool, as it stands out compared to similar products. The primary objective of acquiring Falcon Complete is to identify threats proactively and understand their operating model to improve the ability to detect and respond to their actions. In particular, the solution offers threat intelligence reports tailored to the client's needs and provides a dedicated analyst for real-time support.

USD should acquire Falcon Complete in the next three months and start consuming and sharing Crodwstrike's intelligence reports with the Detection and Response teams as soon as they become available. The University should complete the installation of agents and integration with existing security monitoring tools within the next 12 months.

Total Cost of Ownership (TCO) and Return on Investment (ROI) Analysis

According to Pape (2021), the Total Cost of Ownership (TCO) of implementing Falcon Complete is approximately $1,739,221. This value includes license fees, implementation, and administration costs for 7,500 endpoints. As licensing is responsible for over 30% of the cost, the primary risk is underestimating the number of endpoints. Performing a pre-assessment to identify the assets that should have the solution installed in advance might mitigate this risk, reducing the TCO by at least 10% (Pape, 2021, p. 22).

The ROI can be realized in less than three years at a 109% rate. The savings associated with the implementation of the product come from two factors: reducing downtime in affected hosts reducing fees related to security incidents, as shown below:

Reducing downtime in affected hosts. Pape (2021) proposes that savings associated with downtime prevention are, on average, $140,000 per year.

Reducing fees associated with security incidents. IBM's *Cost of a Data Breach Report 2021* (2021, p. 8) suggests that a breach may cost up to $ 4,800,000 in fees, including legal support, incident response specialists, and fines. Assuming that Falcon could prevent one breach in three years, the total savings would be $3,280,779.

Enforce The Use Of Multifactor Authentication (MFA)

Ransomware groups may reuse leaked credentials and gain access to systems without multifactor authentication. Remote access to the environment and administrative access to specific systems should require an additional level of authentication before users can connect to resources. Furthermore, forcing the use of MFA limits the threat actor's ability to reuse credentials compromised during password guessing attacks.

USD should enforce MFA in 100% of its remote access systems (including VPN, virtual desktops, and webmail) in the next six months.

Establish Robust Backup Procedures

USD must ensure periodic read-only backups of critical systems and data. The backups must be tested to perform sanity checks and ensure that systems can be quickly restored to a clean state. USD should maintain a clean image of servers and workstations that can be restored as soon as possible.

The University should review the existing backup plan in the next three months. The first test should occur in the next six months, and a revision of the backup plan should happen in the next twelve months.

Develop a Data Protection Plan

Ransomware groups target primarily unencrypted data, such as student PII. USD should develop a plan to protect data at rest, in transit, and use, using a combination of data protection policy, encryption, and data loss prevention technology.

USD should detect sensitive information present in the university systems in the next three months. Once the university inventory vital data (including those with privacy implications) utilized by all departments, the cyber security team must classify and label data according to its criticality, deploying policies controls to detect and alert unauthorized access. USD should also educate users to handle the information according to its classification and monitor the deviation of established policies.

Ensure The Network Is Segmented Correctly

Segregating the environment according to the system's requirements and user's roles helps restrain the threat actors' ability to move laterally and limit the impact of ransomware attacks. Network segmentation helps reduce the attack surface of critical systems by restricting the attackers' ability to reach out to their services. Limitations should include preventing users in the corporate network from accessing resources on a network processing sensitive data and restricting remote access traffic only to authorized users.

Assess And Improve USD’s Cyber Hygiene

Null (2021) argues that "by practicing cyber hygiene, organizations strengthen their security posture and can more effectively defend themselves against devastating breaches." That

includes assessing and improving asset management, defining and enforcing secure baselines, and limiting privileges and software usage on systems. Strong hardening procedures and maintaining a robust vulnerability management process help reduce the attack surface that threat actors can exploit to compromise critical systems.

USD should start mapping an inventory of assets supporting all business processes in the next three months. As the University identifies the underlying technologies associated with them, USD should develop a secure configuration baseline to harden the assets and reduce the University's attack surface. USD should evaluate 75% of its systems against the defined baselines and take corrective actions in 18 months.

Conclusions And Next Steps

Ransomware groups continue to evolve and become more organized and sophisticated. Despite most groups' efficiency, USD can still delay and detect these actors and minimize the impact of a security incident. Most threats to the University utilize similar tactics, techniques, and procedures and can be stopped by fundamental security countermeasures.

USD should consider implementing the proposed initiatives following the proposed timeline, which will help the University prevent threats early in the attack cycle and reduce the possibility of compromising sensitive information during an incident.

References

Barrett, B. (2020, February 10). *How 4 Chinese Hackers Allegedly Took Down Equifax*. WIRED. https://www.wired.com/story/equifax-hack-china/

Bracken, B. (2021, December 22). *PYSA Emerges as Top Ransomware Actor in November*. Threatpost. https://threatpost.com/pysa-top-ransomware-november/177242/

Chinese Hackers Charged in Equifax Breach — FBI. (2020, February 10). FBI. https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

Cost of a Data Breach Report 2021. (2021). IBM. https://www.ibm.com/security/data-breach

CrowdStrike Threat Intel Team. (2021, May 28). *DarkSide Pipeline Attack Shakes Up the Ransomware-as-a-Service Landscape*. CrowdStrike. https://www.crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/

Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), & Multi-State Information Sharing and Analysis Center (MS-ISAC). (2020, December 10). *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*. US-CERT. https://www.cisa.gov/uscert/ncas/alerts/aa20-345a

FBI National Press Office. (2021, May 10). *FBI Statement on Compromise of Colonial Pipeline Networks — FBI*. FBI. https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

Federal Bureau of Investigation (FBI). (2021, March 16). *FBI Flash Alert: Increase in PYSA Ransomware Targeting Education Institutions [CP-000142-MW]*. Internet Crime Complaint Center (IC3). https://www.ic3.gov/Media/News/2021/210316.pdf

Foresman, B. (2020, February 26). *Ryuk ransomware shuts down New Mexico school district a second time*. EdScoop. https://edscoop.com/ryuk-ransomware-shuts-down-new-mexico-school-district-second-time/

Government Accountability Office. (2018, August 30). *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. Government Accountability Office. https://www.gao.gov/products/gao-18-559

Lindblom, A. (2021, July 19). *Shlayer Malware: Continued Use of Flash Updates*. CrowdStrike. https://www.crowdstrike.com/blog/shlayer-malvertising-campaigns-still-using-flash-update-disguise/

Milenkoski, A. (2021, September 27). *Threat Analysis Report: Inside the Destructive PYSA Ransomware*. Cybereason. https://www.cybereason.com/blog/threat-analysis-report-inside-the-destructive-pysa-ransomware

Null, C. (2021, August 5). *What Is Cyber Hygiene and Why Does It Matter?* Tanium Endpoint. https://endpoint.tanium.com/what-is-cyber-hygiene-and-why-does-it-matter/

Pape, G. (2021). *The Total Economic Impact Of CrowdStrike Falcon Complete*. Forrester. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021ForresterTEIFalconComplete.pdf

Romo, V. (2021, May 11). *Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack*. NPR. https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack

2021 Data Breach Investigations Report. (2021). Verizon. https://www.verizon.com/business/resources/reports/dbir/

Willey, J. (2020, October 15). *Sheldon ISD forced to pay nearly $207K after hackers targeted servers*. ABC13. https://abc13.com/sheldon-isd-ransom-school-district-hacking-from-hackers-online/7036662/