VACANCY ANNOUNCEMENTS: AN UNACKNOWLEDGED SECURITY RISK

by
Drew Mesa

A research study submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August, 2021

Abstract

Do current U.S. job listings create vulnerabilities to private industries seeking to hire new talent? The hypothesis of this research study argues that many vacancy announcements present informational, organizational, and personnel vulnerabilities to the hiring companies. In a policy-oriented case study review of seventy vacancy announcements, the study determined six job listings across three industries—energy, healthcare, and aviation—contained information that could reveal sensitive trade secrets. These listings posed informational and organizational vulnerabilities to these six organizations, with varying levels of risk and threat. No vulnerabilities towards personnel were found in any job announcement. The hypothesis is disproven, as less than 9% of job postings reviewed were found to have created security risks to companies. This small percentage of the total announcements reviewed indicates that only a minuscule minority of the tens of thousands of vacancy announcements online contain potential vulnerabilities: the problem is not widespread. These conclusions, however, may be disproven with a larger sample size analyzing dozens of U.S. economic industries and hundreds—or thousands—of vacancy announcements. Despite this low statistic, U.S. private industry and companies around the world should begin to consider job listings as another potential information security risk, given the number of state and non-state actors seeking to exploit corporate data.

Advisor: Sarah Clark

Reader: Stephen M. Grenier

Acknowledgements

I wish to thank my parents, grandfather, sister, and close friends for supporting me throughout my two years at Johns Hopkins. Their continuous encouragement has allowed me to balance work and school during the most difficult of times. My mother has served as my reviewer for countless papers and projects these past two years, and I would not be nearly as successful in my studies without her suggestions and feedback. I also wish to extend my gratitude to my work supervisor, Heather, who planted the seed for this research study last year.

Table of Contents

List of Tables

List of Figures

1. Introduction

In today's world, interconnectedness and information sharing has blossomed. As globalization spurs the formation of transnational relationships, the sharing of money and information across borders has increased exponentially. This need for information has catalyzed espionage and cybercrime efforts by both national governments and non-state actors, mainly private corporations, to illegally obtain sensitive data for their own benefit. Private industry has not been immune to these threats; companies have implemented a variety of stringent security measures to ensure sensitive trade secrets remain protected. The challenging security environment facing private businesses across the U.S. has accelerated hiring efforts in the information technology (IT) and security career fields. Many of these hiring efforts are conducted through use of online job postings. How do vacancy announcements pose security vulnerabilities and risks to private organizations? This research question is important, as most companies focus efforts on seeking to prevent unauthorized information disclosures and to secure existing trade secrets from exploitation or exfiltration by malevolent actors, there has been scant government or scholarly research devoted to understanding the risks presented by non-sensitive information, including job listings. With thousands of vacancy announcements posted daily on hundreds of job websites, it is likely that those announcements displaying vulnerabilities will constitute only a very small percentage of advertised vacancies in an Internet replete with vacancy announcements. Notwithstanding the small numbers of problematic vacancy announcements, those that do have vulnerabilities should be taken seriously, especially in an age when information is available to anyone with a network connection.

Craig Scott, in his text on secretive organizations, asserts that some companies devote many resources to promoting themselves and their membership.[1] In many ways, this argument can be extended to vacancy announcements, given the presentation of large amounts of information within each online post. Job listings equate to a tradeoff of providing in-depth information about a company and job duties, which can create vulnerabilities, in exchange for hiring qualified and capable employees. The substantial amount of non-sensitive information within vacancy announcements may offer a level of detail that could create risks to a private company if collated or used to perform target research. As global competition catalyzes technological innovation and economic modernization in countries both large and small, vacancy announcements can provide adversaries a readily available, ubiquitous, and easy platform to gain foundational understandings of a company strategy or product, resulting in risk to an organization's information, organization, and personnel.

2. Background

Hiring organizations use job listings to recruit candidates for positions in a fair and transparent manner.[2] Most postings detail the knowledge, skills, and abilities (KSAs) that applicants need to be successful in their duties. Federal vacancy announcements are mandated to include a position description that indicates job title, salary, location of employment, the name of the recruiting agency, information on how to apply, and a statement regarding equal employment opportunity.[3] Private companies' job listings often also include this same information. In this

[1] Craig Scott, *Anonymous Agencies, Backstreet Businesses, and Covert Collectives: Rethinking Organizations in the 21st Century* (Stanford: Stanford University Press, 2018), x.
[2] U.S. Merit System Protection Board, *Help Wanted: A Review of Federal Vacancy Announcements* (April 2003), 2, https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=253634&version=1831327&application=ACROBAT.
[3] Ibid., 4.

research study, the terms vacancy announcements, job listings, and job postings will be used interchangeably to describe online mechanisms utilized to recruit qualified individuals.[4] Little research has been produced investigating the vulnerabilities of vacancy announcements; therefore, the literature review will focus on the methods businesses use to protect trade secrets. Reviewing the myriad ways companies safeguard data can assist this study in developing potential policy solutions to mitigate the risks to corporate information posed by job listings.

2.1 Defining Trade Secrets

To understand the methods that companies use to protect trade secrets, one must understand the differences between trade secrets and confidential information. A trade secret is information that derives its actual or potential economic value from not being known. Companies work to protect trade secrets from competitors who cannot legitimately obtain the information.[5] All trade secrets are considered confidential information, but not all confidential information consists of trade secrets. Confidential information is defined as information of a sensitive nature that is kept private by the individual or company creating it.[6] Trade secrets are also different from patents. Patents are legal restrictions that grant patent holders' control over information. A trade secret, in contrast, does not offer protections and can be legally used by a competitor if the information—formerly a trade secret—was discovered during a lawful research and development process.[7] Trade secrets can include any of the following: customer lists, contract information,

[4] Ibid.
[5] "Trade Secrets Policy," *U.S. Patent and Trademark Office*, February 7, 2019, https://www.uspto.gov/ip-policy/trade-secret-policy.
[6] *Food Marketing Institute v. Argus Leader Media*, 588 U.S.1, 5 (2019).
[7] D.S. Sengar, "Protection of Trade Secrets and Undisclosed Information: Law and Litigation," *Journal of the Indian Law Institute* 53, no.2 (2011): 259, https://www.jstor.org/stable/43953505.

vendor information, future marketing plans, business strategies, personal employee information, technological processes, and financial records.[8]

2.2 History of Trade Secret Law and Legislation

While companies in the U.S. have produced trade secrets for many generations, legal efforts to protect secretive business information dates back only 120 years. Laws concerning trade secrets began to develop in the 19th century as derivations of state civil liability cases.[9] States courts became increasingly involved in trade secret rulings in the 20th century, resulting in the 1939 "Restatement of Torts" by the American Law Institute. Two sections within this document included an early definition of trade secrets and their misappropriation.[10] The Trade Secrets Act of 1948 represented the U.S. federal government's first foray in attempting to protect confidential business information. The Act prohibited federal employees and contractors from disclosing confidential government information. The statute, however, did not apply to state or local governments, nor to private industry.[11] With federal law limited in its applicability, liability cases involving trade secrets continued to be prosecuted in state courts under an eclectic mix of state legislation. In 1979, the Uniform Trade Secrets Act (USTA) was developed by the National Conference of Commissioners on Uniform State Law to standardize trade secret legislation across all 50 states.[12]

---

[8] Clifford Koen Jr. and Brian London, "To Catch a Thief: Protecting Proprietary Information Including Trade Secrets From Corporate Espionage," *The Health Care Manager* 38, no.4 (2019): 333, https://pubmed.ncbi.nlm.nih.gov/31663872/.

[9] U.S. Congressional Research Service, *Protection of Trade Secrets: Overview of Current Law and Legislation*, by Brian Yen, report R43714 (Washington, DC, 2016.), 4, https://fas.org/sgp/crs/secrecy/R43714.pdf. As legally defined, a tort is an act or omission that causes damage to another party and results in a civil liability. "Legal Information Institute: Tort," *Cornell Law School*, accessed June 15, 2021, https://www.law.cornell.edu/wex/tort.

[10] Ibid.,5.

[11] Ibid., 7.

[12] Ibid., 6.

The federal government remained mostly removed from trade secrets legislation after the implementation of the 1948 Trade Secrets Act; however, this did not mean the U.S. government remained unaware of the growing theft of trade secrets by international actors. The federal government took a major step in its involvement of protecting trade secrets, with the passage of the Economic Espionage Act (EEA) of 1996. EEA, for the first time, made it a criminal offense to steal economic information on behalf of a foreign state actor or a private entity.[13] For 20 years, EEA represented the federal government's most significant contribution to protecting trade secrets and prosecuting wrongdoers, until 2016. That year, Congress passed the Defend Trade Secrets Act, which provided a uniformed federal statute in prosecuting both government and private industry trade secret cases, allowing private companies to pursue their cases in federal courts rather than state courts.[14]

Despite the relatively recent federal laws designed to prevent theft of trade secrets by foreign institutions and to allow federal prosecution of trade secrets cases, the contemporary legal environment is still dominated by state prosecution of civil actions. Every U.S. state currently has laws governing the protection of trade secrets from theft or disclosure. The USTA has been effective at standardizing state intellectual property or trade secret statutes, with 48 states having adopted the measure.[15]

---

[13] Ibid., 7.
[14] "Explaining the Defend Trade Secrets Act," *American Bar Association*, September 20, 2016. https://www.americanbar.org/groups/business_law/publications/blt/2016/09/03_cohen/.
[15] U.S. Department of Commerce, Patent and Trademark Office, *Trade Secret Protection in the United States*, https://www.nist.gov/system/files/documents/mep/marinaslides.pdf.

2.3 Current Threat Environment

State and federal governments implemented these statutes in direct response to an everchanging threat that witnessed a multitude of vulnerabilities exploited at all levels of government within the United States and private industry. Private companies can obtain intelligence on competitors legally using open-source research to uncover press releases, public documents, and social media posts to predict the future behavior of competitors and position themselves favorably within a market.[16] The U.S. is a global hub of research and development activities, creating an enticing target for foreign actors.[17] Annual theft of intellectual property from U.S. companies is estimated to result in losses of around $300 billion.[18] One reason foreign governments steal corporate trade secrets is to facilitate expeditious development of military technology. Private foreign entities can also exploit trade secrets by using illegally obtained research and development information to reduce costs of existing products, reallocating the conserved funds to other ventures.[19] With foreign actors now viewing domestic private enterprise as extensions of the government, state-sponsored corporate espionage is on the rise. Countries now believe the act of stealing U.S. corporate secrets as imperative to improving both economies and foreign relations.[20]

---

[16] Josh Fruhlinger, "What is Corporate Espionage? Inside the Murkey World of Private Spying," *CSO Online*, July 2, 2018, https://www.csoonline.com/article/3285726/what-is-corporate-espionage-inside-the-murky-world-of-private-spying.html.

[17] U.S. Office of the Director for National Intelligence, National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (July 2018), 4, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[18] Lorrand Laskai and Adam Segal, "A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage," *Council on Foreign Relations* (December 2018): 2, https://www.cfr.org/report/threat-chinese-espionage.

[19] European Union's Institute for Security Studies, *The Threat of State-Sponsored Industrial Espionage*, by Massimo Pellegrino (Paris, France, 2015), 1, https://www.iss.europa.eu/content/threat-state- sponsored-industrial-espionage.

[20] Bill Priestap and Holden Triplett, "The Espionage Threat to U.S. Business," *Lawfare*, October 1, 2020, https://www.lawfareblog.com/espionage-threat-us-businesses.

As the scale of foreign threats to U.S. businesses grows, information is being compromised through several methods, including supply chain penetrations, cyber hacks, human-enabled data exfiltration, and social media exploitation. Penetration of U.S. supply chains has become easier in recent years, as globalization has driven companies to produce many technological components overseas. These overseas production facilities can be infiltrated by foreign adversaries through either physical or electronic means. Global supply chains can be compromised at multiple points— the design, manufacture, deployment, and continued maintenance phases of a product.[21] Additionally, the large amount of foreign technology in U.S. goods creates numerous vulnerabilities within U.S. private companies; such components can be used to infiltrate other products or services.[22] The targeting of U.S. industry through the cyber domain by foreign adversaries—state and non-state actors—has risen exponentially over the past two decades.[23] The advent of artificial intelligence (AI) and the Internet of Things (IoT) has only compounded the threats already facing U.S. corporate industries.[24] AI and the IoT allow additional avenues through which foreign actors can steal information. The 2020 SolarWinds hack exemplifies the danger facing the United States. Russian intelligence services used malicious code in a software update to compromise nearly one hundred private companies and dozens of federal agencies.[25] Additionally, foreign intelligence agencies are increasingly using social media applications to target and recruit unwitting individuals. For example, the Chinese government has used job networking site LinkedIn to recruit individuals to provide sensitive

[21] U.S. Office of the Director for National Intelligence, National Counterintelligence and Security Center, *National Counterintelligence Strategy of the United States of America 2020-2022* (February 2020), 7, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.
[22] Ibid.
[23] Pellegrino, *Industrial Espionage*, 1.
[24] National Counterintelligence and Security Center, *Foreign Economic Espionage,* 4.
[25] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *NPR*, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

U.S. government or business information, under the cover of corporate exchanges or consulting opportunities.[26] Despite the rise in cyber threats, human penetrations of U.S. companies remain a pervasive issue. Foreign intelligence entities and state-connected private corporations have been known to place human assets in U.S. academia, research labs, and innovative industries.[27]

2.4 Foreign Threat Actors

The People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and even U.S. allies are the state actors most engaged in the theft of U.S. trade secrets through supply chain, cyber, or human penetrations. The close relationship between Chinese private enterprise and the Chinese national government,[28] has made China a formidable adversary in the theft of commercial trade secrets. Science and technological data are the most valuable information to the Chinese government, as it seeks to modernize its military to reach strategic parity with the United States.[29] In 2020, cleared government contractors reported that 40% of all information collection incidents originated from East Asian and Pacific countries.[30] China's next-generation stealth fighter exemplifies its economic espionage efforts for military purposes: The design for the U.S. F-35 stealth fighter were stolen from contractor BAE in 2009 and reverse-engineered into a Chinese fighter of similar design.[31] Why do U.S. companies continue to engage in local manufacturing partnerships within China given this threat? It is a tradeoff between security and profit. China represents a $500 billion market for U.S. companies,

---

[26] Edward Wong, "How China Uses LinkedIn to Recruit Spies Abroad," *New York Times*, September 27, 2019, https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.
[27] Ibid., 8.
[28] Pellegrino, *Industrial Espionage*,1.
[29] National Counterintelligence and Security Center, *Foreign Economic Espionage,* 5.
[30] U.S. Defense Counterintelligence and Security Agency, *Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry* (December 2020), 7, https://www.dcsa.mil/Portals/91/Documents/CI/2020-Targeting-US-Technologies_Briefing.pdf.
[31] Pellegrino, *Industrial Espionage*,2.

promising large revenue gains and profits, if U.S. companies manufacture products in China. Furthermore, the Chinse government, in some cases, has imposed large tariffs of U.S. goods—such as automobiles—imported into the country, if produced without a domestic partner.[32]

Much like China, the Russian Federation undertakes state-sponsored economic espionage to promote its economy. The Russian government, and its non-state proxies, engage in state-sanctioned targeting activities against private corporations to advance state interests and enable modernization of domestic industries.[33] The misappropriation of trade secrets is an important pillar in Russia's revival of its contracted economy, especially the rebuilding of its military industries. U.S. technology continues to play a crucial role in the diversification of the Russian economy.[34]

The Islamic Republic of Iran follows Russia's model of using economic espionage to spur economic growth. Iran conducts espionage and infiltration operations against U.S. companies to gain information that will benefit domestic businesses and modernize its antiquated military. The acquired U.S. information is used to stimulate the Iranian economy by catalyzing foreign sales of new—stolen—technologies and encouraging diversification away from oil production.[35] While Iran may be portrayed as a country crippled by international sanctions and lack of modern technologies, its intelligence services represent a serious threat to the United States. Between 2013-2017, nine Iranian nationals working for the state-affiliated Mabna

[32] Daniel Shane, "How China gets what it wants from American Companies," *CNN Money,* April 5, 2018, https://money.cnn.com/2018/04/05/news/economy/china-foreign-companies-restrictions/index.html.
[33] Ibid., 2.
[34] National Counterintelligence and Security Center, *Foreign Economic Espionage,* 8.
[35] Ibid., 9-10.

Institute, infiltrated the accounts of 8,000 university professors across the world, compromising research worth $3.4 billion.[36]

Targeting U.S. corporations for valuable trade secrets is not an exclusive activity of adversarial nations or non-state actors, but of U.S. allies as well. Former Defense Secretary Robert Gates has labeled France as one of the most prolific actors involved in corporate espionage. He notes that the French intelligence services routinely enter hotel rooms occupied by U.S. businesspeople to copy information from laptops. This information is then passed onwards to French companies for exploitation.[37] Currently, allied nations continue to use their unique access and privileged status to engage in economic espionage against U.S. corporations for their own gain.[38]

2.5 Review of the Literature

With a broad mix of foreign actors conducting operations against private companies, U.S. industries have used many strategies, including restrictive clauses, employee training, physical security measures, and cybersecurity to protect information. Richard Epstein argues that restrictive clauses are contractual obligations developed by owners or organizations to enforce confidentiality and include need-to-know principles and limits on the transfer of information to

[36] U.S. Department of Justice, Office of Public Affairs, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," press release, March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

[37] Philip Ewing, "Gates: French Cyber Spies Target U.S.," *Politico*, May 22, 2014, https://www.politico.com/story/2014/05/france-intellectual-property-theft-107020.

[38] U.S. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage* (October 2011),6, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

third parties.[39] D.S. Sengar asserts that the most common type of restrictive document is the non-disclosure agreement (NDA), which bars employees from disclosing confidential information to competitors.[40] Clifford Koen Jr. and Brian London take a more expansive view of these clauses, arguing that employers can also use non-compete clauses, non-solicitation clauses, and non-recruitment stipulations to further prevent information leaks. Non-compete clauses prevent employees from doing business with a competitor for a specific period of time after departure.[41] A non-solicitation requirement blocks departing employees from soliciting the vendors or customers of former employers.[42] Non-recruitment stipulations prevent competing companies from hiring current employees.[43] Rick Richmond and Sandra Hanian contend that restrictive clauses are not isolated to legal documents, such as NDAs, but also include licensing agreements. They argue these agreements allow companies to ensure information is being properly handled by vendors to prevent compromise.[44]

Most companies use restrictive clauses to ensure information protection after an employee departs a business, but employee training in proper security measures can facilitate the protection of trade secrets during an individual's employment. Premkumar Chitalutu and Ravi Prakash state that private companies routinely use security training to educate employees on

[39] Richard Epstein, "The Constitutional Protection of Trade Secrets Under the Takings Clause," *University of Chicago Law Review* 57 (2004): 60, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2200&context=journal_articles.
[40] Sengar, "Law and Litigation," 264.
[41] Koen Jr. and London, "To Catch a Thief," 334.
[42] Ibid., 335.
[43] Ibid.
[44] Rick Richmond and Sandra Hanian, "Protecting Trade Secrets in Government Contracting," in *Government Contracting Law Report* 4, no.3, 72-76. (New York: LexisNexus,2018), 75, https://jenner.com/system/assets/publications/17827/original/Rick%20Richmond%20and%20Sandra%20Hanian.pdf?1520963384.

information security policy and what activities are, or are not, permissible.[45] Marko Gabric also asserts that security training is used by organizations to teach security policies and protect data.[46] Melanie Reid takes a different approach to security training, contending that such methods are meant to educate employees on threats and procedures to follow if approached by a competitor or foreign intelligence service seeking information.[47]

Protection of trade secrets by a properly trained workforce can be enhanced by use of physical security, Koen Jr. and London explain that companies use locking mechanisms, signs, document markings, and policies limiting removal of information from buildings to protect sensitive information.[48] Gabric agrees and includes good lighting, fences, guards, X-ray machines, and closed-circuit television as protective mechanisms.[49]

Protection and security through the cyber domain complement the use of physical security systems to protect physical documents and trade secrets. Koen Jr. and London state that the most common electronic controls used by private industry are firewalls, computer access codes, strong passwords, and software to prevent unauthorized copying.[50] There is a noticeable divergence in the literature when it comes to using tracking systems as a cyber security tool. Richmond and Hanian contend that companies use tracking systems only to keep tabs on

---

[45] Premkumar Chitalutu and Ravi Prakash, "Organizational Security Policies and Their After Effects," in *Information Security and Optimization*, eds. Rohit Tanwar, Tanupriya Choudhury, Mazdak Zamani, and Sunil Gupta (Baton Rouge, LA: CRC Press, 2020), 53,https://www.taylorfrancis.com/books/edit/10.1201/9781003045854/information-security-optimization-rohit-tanwar-tanupriya-choudhury-mazdak-zamani-sunil-gupta.

[46] Marko Gabric, "Incorporating Security Elements," *in Corporate Security Management, Challenges, Risks, and Strategies* (Oxford, UK: Butterworth Heinemann, 2015).

[47] Melanie Reid, "A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? Effectively Dealing With This Global Threat?" *University of Miami Law Review* 70 (2016): 828, https://repository.law.miami.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4468&context=umlr.

[48] Koen Jr. and London, "To Catch a Thief," 334.

[49] Gabric, "Incorporating Security Elements."

[50] Koen Jr. and London, "To Catch a Thief," 334.

information as it is used, noting any unpermitted copying or dissemination.[51] However, Iosif Androulidakis and Emmanouil Kioupakis disagree, claiming that companies use tracking systems to verify incidents in order to pass such information onwards to law enforcement,[52] rather than simply tracking information usage.

2.6 Limitations of Existing Research

The background information and literature provide insights into the contemporary espionage threats facing corporate industry and how private businesses protect their trade secrets; however, there is a dearth of coverage concerning contemporary economic espionage by U.S. allies (with most stories dating back 10 or more years), and how companies respond when faced with a compromise of information. Most of the literature dedicates itself to the methods used to protect against theft, without revealing what companies can do, or have done, to mitigate compromises after they occur. The main shortcoming of the literature as it concerns this topic is that there is no documentation published on either the security risks created by vacancy announcements or the variables that malicious actors analyze within job listings to glean sensitive information from. Most of the information that has been produced by government and academia concerns the dangers to trade secrets companies already possess; it does not account for the impacts of public information posted online by hiring organizations, which may be harmless, but when combined with additional open-source research or data aggregation, can prove threatening.

[51] Richmond and Hanian, "Protecting Trade Secrets,"75.
[52] Iosif Androulidakis and Fragkiskos – Emmanouil Kioupakis, *Industrial Espionage and Technical Surveillance Counter Measures* (Switzerland: Springer International, 2016), https://www.springer.com/gp/book/9783319286655.

2.7 Policy Implications and Research Contributions

The current policy environment protecting trade secrets from compromise is inadequate in mitigating the threats from state-sponsored malicious actors. Most concerning is the lack of federal or state guidelines that explicitly define how trade secrets are to be protected. This hands-off approach, leaving the methods of protecting trade secrets up to individual companies, has led to varying levels of security across industries and has facilitated exploitation and exfiltration of secrets from unsecure vulnerability points. Furthermore, most of the contemporary collaboration between the U.S. government and private industry concerning information security remains centered on the protection of trade secrets produced by entities. This focused attention on protecting sensitive information has led to a dearth of analysis of the threats posed by non-sensitive information produced and released by companies, whether in press releases, vacancy announcements, or quarterly reports.

This research project will contribute to the existing body of literature by analyzing risks to hiring organizations during the pre-hire process, as job postings are used to recruit qualified individuals. This will compliment what has been previously written concerning training of new employees to safeguard trade secrets, protection of information through various physical and electronic mechanisms once an employee enters on duty, and restrictive clauses governing behavior after an employee departs from a company. By conducting this research, the risks to trade secrets will be detailed and assessed through the entire human resources process: pre-hire, entrance on duty, maturation in the workplace, and departure or retirement.

3. Hypothesis

I hypothesize that job postings and vacancy announcements advertised by U.S. private companies pose informational, organizational, and personnel threats to these organizations. These information risks include position descriptions, job duties, and KSAs that are presented within a posting to gain the most qualified candidates. These components convey specific information to individual applicants, but can also clue adversaries into potentially sensitive job functions or future company plans. Organizational vulnerabilities within a job listing can include location information, including physical addresses. This geographic data may allow the correlation of activities, such as research and development, to a specific location, creating a potential physical security issue. Personnel vulnerabilities can be generated through the inclusion of contact information—work e-mail addresses and phone numbers—for hiring managers or human resources employees. This work-related data connects an individual to a specific set of job duties. The linkage of individual contact information and job duties can facilitate the targeting of additional employees by a foreign adversary for recruitment.

3.1 Methodology

This project engages in a policy-oriented case study comparison of multiple companies across different industrial sectors. The cases in this project are not represented by each individual vacancy announcement but, rather, the industry under which companies are categorized. The aviation, healthcare, and energy sectors represent the three comparative cases being studied, each with multiple vacancies and various companies grouped under each case. These three cases were chosen given the current technological developments occurring within each industry, and the

prevalence of foreign adversaries that target these critical sectors to obtain valuable data. Individual vacancy announcements under a specific case include both mainstream and start-up companies—incorporating conventional and experimental technologies, plans, and strategies—allowing comparisons across a wide array of job data. The study reviews seventy total vacancy postings. All vacancies that contain detailed technical information, key words—such as "confidential" or "proprietary" within the announcement or associated websites, company-specific processes and acronyms, or location information, are subject to additional research to determine if such data truly poses a vulnerability. This preliminary research involves consulting scholarly research and news articles to determine if said information presented within a job listing has been compromised or is vulnerable to compromise. Those listings determined to have problematic information, through inclusion of detailed technical jargon or specified internal processes within the announcement, will be thoroughly analyzed and discussed, while those that do not will merely be tallied. All vacancies reviewed are recorded by title to obtain a percentage of the number of potentially risky job announcements to those that are harmless. This number should not be taken as representative of the entirety of job postings on the Internet, merely a statistical representation for this study only.

While it is expected that some level of detail provided in a vacancy announcement will highlight vulnerabilities or potentially sensitive information, the hypothesis will only be confirmed if a statistical majority of job listings reviewed contain information that created vulnerability or risk to an organization. Selection bias is prevented by reviewing all companies represented within a specific industrial case; no preference will be given to companies based on their size or advertised position titles (e.g., reviewing company X because it has more open IT

security positions than company Y). The only prerequisite for inclusion is that both the company and position be located within the United States.

3.2 Terms and Definitions

Vacancy listings determined to contain vulnerabilities will be ranked using scales of both threat and risk—from low to high. For this study, threat is defined as an individual or incident with a potential to adversely impact a company. Threat will be measured by compiling stories and articles discussing real-world compromises or attacks against similar technology or products referenced in a job posting. Vulnerabilities encompass qualities within companies that facilitate conditions favorable to threats.[53] Vulnerabilities will be measured by analyzing vacancy announcements for detailed descriptions of duties, skills, or locations that allow visibility into the internal agendas of private companies and/or products. Key words included in either announcements or company websites, such as "proprietary" or "confidential" will be logged. The use of key words will be used to target companies using an adversarial mindset, as inclusion of such vocabulary draws additional attention. Risk entails the measurement of threats towards companies given their impact and possibility of occurring.[54] Risk will be analyzed by determining if recent threats have to potential to adversely impact a company and, if so, the severity of those impacts.

[53] U.S. National Aeronautics and Space Administration, *Information Technology Threats and Vulnerabilities*, accessed June 2021, https://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm.
[54] U.S Department of Commerce, National Institute of Standards and Technology, *Guide for Conducting Risk Assessments: Information Security* (September 2012), 6, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Table 3.2.1. Measuring Threat (Table by Author).

Severity	**Explanation**
Low	No instances of previous compromises of similar information, data, or systems specified in a vacancy announcement.
Moderate	Compromises have occurred involving information or systems similar—although not the same—as those specified in a vacancy announcement.
High	Information or systems detailed in a vacancy announcement have been previously exploited or compromised

Table 3.2.2. Measuring Risk (Table by Author).

Risk Level	**Explanation**
Low	Compromise has no impact on a company's future financial growth, operations, or planning.
Moderate	Compromise has limited impacts to company finances, operations, or plans.
High	Disclosure puts company at risk of major financial losses, substantial halts to operations, or severely disrupts long-term plans.

4. Data

4.1 Energy – ExxonMobil

The energy sector of the United States is experiencing a transformation, as energy regulators, power production companies, refiners, and producers move away from fossil fuels and embrace renewable energy, battery technology, and nuclear power—fission and fusion. With this new global push away from polluting fuels, ExxonMobil, one of the world's largest oil and gas

production companies, faces a dilemma as it enters a potentially uncertain future. Despite the energy transition, ExxonMobil has publicly reinforced its position on upgrading existing oil and gas infrastructure, launching the "Growing the Gulf" initiative in 2017. This campaign has seen the company invest money into its Gulf Coast facilities— oil refineries and chemical manufacturing plants—to increase production capacity and export capabilities.[55]

Given the ongoing initiative modifying and improving facilities along the Gulf Coast, ExxonMobil posted a job advertisement on May 21, 2021, for an "HR Senior Manufacturing Professional." The announcement states that the selectee would work directly in labor relations and develop talent management strategies for Exxon employees. In the post, "delivering change management plans" was listed as a crucial "job role responsibility."[56] Houston, Texas, is listed as the primary location of the position; however, the job listing notes that Baytown, Texas; Baton Rouge, Louisiana; Beaumont, Texas; and Joliet, Illinois are alternative locations.[57]

The multiple duty locations advertised within the announcement in Louisiana, Texas, and Illinois are currently undergoing modifications that indicate the company's future production of oil-based products—as indicated by open-source research. The concept of change management in the oil and gas sector involves the transformation of an organization or its operations to sustain business and "remain competitive in a volatile environment." [58] Performing research on ExxonMobil's operations at its Baytown Chemical Plant reveals that the facility will undergo a

[55] "Growing the Gulf," ExxonMobil, accessed June 1, 2021, https://corporate.exxonmobil.com/Locations/United-States/Growing-the-Gulf.
[56] "HR Senior Manufacturing Professional," *ExxonMobil*, posted on May 12, 2021, https://jobs.exxonmobil.com/ExxonMobil/job/Houston-HR-Senior-Manufacturing-Professional-TX-77001/747277300/.
[57] Ibid.
[58] I.S. Bahrudin, B. Abdullah, N.A. Mohd Sallh, P. Shariffudin, "A Case Study on Change Management Readiness for an Oil & Gas SME Company in Malaysia" (conference paper, 6th International Conference on Advances in Mechanical Engineering, Kota Kinabalu, Sabah, Malaysia, August 14-16, 2019), 1.

$2 billion upgrade, scheduled to commence in 2022. Baytown is currently the largest integrated petrochemical plant in the United States, refining and producing plastic materials. The future construction will add a new polymer unit to increase the efficiency and quality of polymer products. This new unit will facilitate the company's entrance into the olefin market, allowing it to produce high quality industrial and automotive oils and packaging plastics.[59] Likewise, online sources indicate the Baton Rouge plant is undergoing a $334 million expansion to improve its petrochemical efficiency and production levels by 2023. These improvements and retrofits will result in the plant being able to produce a variety of new products—rubber, adhesives, and isopropyl alcohol.[60] Local reports uncovered in open source research also stated that the Beaumont, Texas, facility also recently completed an expansion of its polyethylene production lines, [61] permitting an 65% increase in production to meet global demands.[62]

4.2 Energy – TAE Technologies

As ExxonMobil defines its future without oil and gas, start-up company TAE Technologies (TAE) is embracing the future through nuclear fusion technology. According to its website, TAE is developing a zero-emissions nuclear fusion reactor, which it describes as

[59] "Exxon Mobil's $2 Billion Baytown Chemical Plant Expansion Continues Permian Basin Growth," *Industry Week*, May 2, 2019, https://www.industryweek.com/leadership/companies-executives/article/22027535/exxonmobils-2-billion-baytown-chemical-plant-expansion-continues-permian-basin-growth. It should be noted that this construction in independent of ExxonMobil's Growing the Gulf Initiative.

[60] Kristen Masbrucker, "ExxonMobil Mulls $334 Million Chemical Facility Expansion in Baton Rouge, Seeks Incentives," *Advocate (*Baton Rouge, LA), March 30, 2021, https://www.theadvocate.com/baton_rouge/news/business/article_9aa51b6e-9176-11eb-a0e3-1f5b6c15f4e9.html.

[61] U.S. Environmental Protection Agency, *Plastics: Material-Specific Data*, accessed June 10, 2021, https://www.epa.gov/facts-and-figures-about-materials-waste-and-recycling/plastics-material-specific-data. Polyethylene is a crucial compound used to produce much of the plastic materials in use around the world, including plastic food packaging containers, bottles, and bags.

[62] Robert Brelsford, "ExxonMobil Commissions Beaumont Polyethylene Expansion," *Oil and Gas Journal*, February 25, 2019, https://www.ogj.com/refining-processing/petrochemicals/article/14036785/exxonmobil-commissions-beaumont-polyethylene-expansion.

proprietary, using accelerators and plasma physics to reduce costs and boost reaction performance.[63] TAE has a goal of delivering commercial nuclear fusion power, with additional objectives of using their technology for power management and life sciences.[64] On May 17, 2021, TAE posted a job announcement for a "Scientist—Modeling Stability and Fast Ion Physics" at its Foothill Ranch, California, location. This vacancy announcement's stated position objectives would be to perform stability and fast ion transport in TAE's proprietary Field Reversed Configuration (FRC) platform. Job duties listed in the announcement include performing numerous technical actions, such as developing computational models for fast ion waves.

4.3 Healthcare – Pfizer

Like the energy industry, healthcare is experiencing rapid change, as health systems around the world modernize and new treatments are developed to combat existing and emerging illnesses. Pfizer, one of the leading global pharmaceutical companies, is heavily involved in new drug development and is constantly seeking to enter new markets. Pfizer's job opening for a "Senior Associate, Contract Management" in Lake Forest, Illinois, posted on June 1, 2021, is focused on assisting the company in formulating drug market strategies. Contracting experience in institutional, oncology, hemophilia, and trade markets is listed under the vacancy announcement's "preferred qualifications" for the position.[65]

---

[63] "Frequently Asked Questions," TAE Technologies, accessed June 5, 2021, https://tae.com/about-us/faq/.

[64] "Scientist—Modeling Stability and Fast Ion Physics," *TAE Technologies,* posted May 17, 2021, https://recruiting2.ultipro.com/TRI1021TRIAE/JobBoard/49386e5d-f909-4648-8335-415ce97e3f15/OpportunityDetail?opportunityId=46f59c3f-f100-4a6a-9316-28fed59b9253.

[65] "Senior Associate, Contracting Management," *Pfizer*, posted on June 1, 2021, https://pfizer.wd1.myworkdayjobs.com/en-US/PfizerCareers/job/United-States---Illinois---Lake-Forest/Senior-Associate--Contract-Management_4814121.

The inclusion of these qualifications, specifically familiarity with oncology and hemophilia markets, provides clues into Pfizer's future market and product development strategy. Conducting web research on Pfizer's hemophilia drug activities indicate that the company is currently in test trials for two new hemophilia drug treatments. Recent news sources reveal the company is developing drug SB-525 with partner Sangamo Therapeutics for gene therapy use in hemophilia A patients; the drug is currently in a trial study phase.[66] SPK-9001 is Pfizer's other collaborative drug treatment for use in hemophilia B patients. It is reported that this new treatment is currently in the early phases of safety testing in both Europe and North America.[67]

The development of Pfizer's two hemophilia treatments indicates the company's aggressive approach to be one of the first drugmakers to enter this emerging market. Pfizer was seen by market analysts as having fallen behind other competitors for hemophilia drugs in getting approvals from the Food and Drug Administration (FDA) to begin full-scale production.[68] News stories in August 2020, however, reported that Pfizer's main hemophilia drug competitor, BioMarin Pharmaceuticals, had its application denied by the FDA for final study approval, pushing its timeline out from 2020 to 2022. Online sources anticipate that Pfizer is expected to start final study trials this year, now giving it a substantial lead over its

[66] "Pfizer, Sangamo dose first participant in phase 3 study of Hemophilia A gene therapy treatment," *Pharmaceutical Business Review*, October 8, 2020, https://www.pharmaceutical-business-review.com/news/pfizer-sangamo-dose-first-participant-in-phase-3-study-of-hemophilia-a-gene-therapy-treatment/.

[67] "Upcoming Potential Advances in the Treatment of Hemophilia," *Ascella Health*, June 2020, https://www.ascellahealth.com/sites/default/files/files/document/june_2020_-_advances_in_hemophilia_treatment.pdf.

[68] Jonathan Gardner, "Pfizer Lays Out Gene Therapy Aspirations," *BioPharma Drive*, January, 28, 2020, https://www.biopharmadive.com/news/pfizer-gene-therapy-phase-3-dmd-hemophilia/571238/.

competitors in being the first to market new hemophilia treatments.[69] Given this information, Pfizer could be looking to hire a contracting associate to advance its drug testing of SPK-9001 into phase 3 clinical trials and bring SB-525 to market using mass production. In a conversation regarding Pfizer's intent to launch three new cures by 2023—totaling $4 billion in revenue potential—Suneet Varma, head of Pfizer's rare disease business, stated that the company was "in an unrivaled position to go to market."[70]

4.4 Healthcare – HCA Healthcare

As Pfizer's experience illustrates, the healthcare industry is extremely competitive, and having proper security to protect information and facilities is imperative to preventing unauthorized access to buildings or sensitive documents. HCA Healthcare's June 2021 job posting for an "Identity and Access Management Security Developer" states the position "would be responsible for the implementation and development of the company's Microsoft Azure Active Directory (AD) hosted identity and access management systems." The announcement stipulates that applicant would be expected to implement these security systems through use of multiple applications, including Microsoft SQL Server and JavaScript.[71]

HCA Healthcare's description of the Azure AD access management system in the job posting immediately exposes the information of a vendor that the company contracts with to protect its information—Microsoft. Further online research reveals that Azure AD is marketed

[69] Caroline Hunter, "U.S. FDA Rejects BioMarin Hemophilia Gene Therapy, Shares Dive," *Reuters*, August, 19, 2020, https://www.reuters.com/article/us-biomarin-pharma-fda/u-s-fda-rejects-biomarin-hemophilia-a-gene-therapy-shares-dive-idUSKCN25F1H6.
[70] Bill Alpert, "How Pfizer Plans to Lead the Industry in Gene Therapies," *Barron's*, September, 16, 2020, https://www.barrons.com/articles/how-pfizer-plans-to-lead-the-industry-in-gene-therapies-51600197117.
[71] "Identity and Access Management Security Developer," HCA Healthcare, accessed on June 3, 2021, Identity and Access Management Security Developer in Nashville, Tennessee, United States (hcahealthcare.com).

by Microsoft as an access and identity management system that incorporates multi-factor authentication and single sign-on capabilities to protect and manage access to company systems.[72] Identity and access management systems are used to identify individuals and verify their system accesses.[73]

4.5 Aviation – Pratt and Whitney

Airplane engine manufacturer Pratt and Whitney (P&W) also includes vendor information in a vacancy posting. P&W's "Global Security Technology Manager" vacancy announcement states the applicant would be responsible for the design and control of facility site security mitigation and technology systems. Key responsibilities listed in the announcement include the development and implementation of physical security access management using the Lenel OnGuard Enterprise system. The job listing provides the actual address of the position: 4000 Main Street, East Hartford, Connecticut, 06118.[74] An Internet search of the position's location reveals that Pratt and Whitney's corporate headquarters shares the same address.[75]

With the physical address of the company ascertained in the job posting, one can understand the relationship between the research and development activities occurring on the campus with its use of Lenel as a vendor for physical security systems. Local news articles indicate that housed on-site at the East Hartford campus is Pratt and Whitney's Engineering and Technology Center, which serves as a global hub for development of the company's commercial

[72] "Azure Active Directory," Microsoft, accessed June 4, 2021, https://azure.microsoft.com/en-us/services/active-directory/.
[73] "What is Identity and Access Management," Cloudflare, accessed June 4, 2021, https://www.cloudflare.com/learning/access-management/what-is-identity-and-access-management/.
[74] "Global Security Technology Manager," *Pratt and Whitney*, posted May 12, 2021, https://jobs.prattwhitney.com/job/east-hartford/global-security-technology-manager/1737/19369400.
[75] "Contact Us," Pratt and Whitney, accessed June 18, 2021, https://prattwhitney.com/company/contact-us.

PurePower and military F135 engines. In an interview, Robert Leduc, president of the company, stated that the campus represents the "nerve center of Pratt and Whitney's…design of the finest commercial and military engines in the world."[76] A review of Lenel's company website details that its OnGuard Enterprise technology is designed for use on multiple facilities dispersed across a large area. According to the website, the system integrates multiple physical security activities under one system: fire alarms, employee ID badging systems, biometric identification technology for doors and exits, closed-circuit television (CCTV) surveillance, door access controls, and computer workstation monitoring.[77] Performing additional research on Lenel's product uncovers partners the company utilizes to create its integrated security system: The CCTV cameras used by OnGuard are sourced from FLIR Systems, Airphone, Amika Mobile Corporation, or Everbridge, among others. The identity management systems use technology developed by Intellisoft, Entrust, Enterprise Security, or Detrios. Employee card readers and biometric systems are procured through agreements with Stanley Healthcare, Alutel, BioConnect, and Sekure ID.[78]

4.6 Aviation – Spinlaunch

Much like P&W, start-up rocket company Spinlaunch releases detailed job descriptions in its vacancy announcement. According to news sources, Spinlaunch has plans to develop a novel orbital launch vehicle system, using a large centrifuge of proprietary design to spin rockets on the ground up to 5,000 mph and 10,000 times the force of gravity. The company has

[76] "PW Unveils New Engineering and Technology Center on its East Hartford Campus," *Pratt and Whitney*, November 11, 2017, https://newsroom.prattwhitney.com/2017-11-11-Pratt-Whitney-Unveils-New-Engineering-and-Technology-Center-on-its-East-Hartford-Campus.
[77] "Integrated Security Management Software," Lenel, last updated 2015, https://www.lenel.com/assets/library/onguard/OG_SS_ENT_0515_new%20format.pdf.
[78] "OAAP Partners and Products," Lenel, accessed June 10, 2021, https://www.lenel.com/solutions/open-integration/oaap/partners-products-search.

publicized plans to launch upwards of five times per day, each at a cost of $500,000.[79] Spinlaunch has been apprehensive about discussing its technology and future strategy in detail, only confirming that it is developing a rocket to support satellite constellations.[80] This lack of confirmation makes the company's job post for a "Senior Satellite Systems Engineer" useful to both industry watchers and foreign competitors. The vacancy announcement states that the position's incumbent would be responsible for developing and managing satellite designs, with an emphasis on standardized satellite buses. Within the announcement, satellite modeling and cost estimates for a "high volume small satellite bus" are listed as additional mission responsibilities. Experience building satellite buses at high volumes, including for SpaceX, Millennium Space Systems, Planet, Skybox, Tyvak, and OneWeb is a desirable skill, according to the job posting.[81]

Spinlaunch's advertisement for a satellite engineer, along with the announcement's mention of a variety of competing space companies, illustrates its publicly unacknowledged aspirations for manufacturing in-house small satellites for its launch vehicles. A review of the websites of the various companies mentioned in Spinlaunch's job listing indicate that all develop small satellite systems for a variety of rockets. Reviewing public information about the companies listed leads to the conclusion that Spinlaunch is planning to develop satellite buses of no greater mass than 200 pounds for imagery or broadband network use.

---

[79] Daniel Oberhaus, "Inside Spinlaunch, the Space Industry's Best Kept Secret," *Wired*, January 29, 2020, https://www.wired.com/story/inside-spinlaunch-the-space-industrys-best-kept-secret/.
[80] Ibid.
[81] Spinlaunch, "Senior Satellite Systems Engineer," accessed June 11, 2021, https://www.google.com/search?client=firefox-b-1d&q=spinlaunch+jobs&ibp=htl;jobs&sa=X&ved=2ahUKEwjsjumPs4nxAhXbF1kFHZ1OBaIQudcGKAJ6BAgDEC4#htivrt=jobs&htidocid=LdYllHflkxd-odkSAAAAAA%3D%3D&fpstate=tldetail .

5. Discussion

5.1 ExxonMobil

The connection of ExxonMobil's advertised senior manufacturing human resources position in developing change management plans and the associated locations in Texas, Louisiana, and Illinois, creates both an informational and organizational vulnerability for the company, as it enables one to uncover its future business strategies for persevering beyond the current period of energy transition through way of recent construction at the sites. While ExxonMobil has remained reticent to discuss its future strategic planning, open-source research indicates that the upgrades to its plants in Texas and Louisiana appear to be evolving the company's production capacities away from traditional gas and oil to petrochemicals, plastics, and other industrial products. These changes, coupled with the knowledge that the goal of change management is to ensure continuing competitiveness in a new environment, lead to the conclusion that ExxonMobil's future strategy is to use oil and gas to produce plastics. As climate consciousness permeates countries around the world, oil producers are increasingly using petroleum to produce plastic feedstocks, according to online research. It is estimated that by 2030, one-third of new oil production growth will be dedicated to producing plastics, which is seen by the fossil fuel industry as a more stable profit stream than oil. ExxonMobil itself has indicated in public statements that plastic production could be a solution to halt falling oil demand.[82]

[82] Ajit Niranjan, "Oil Companies Pivot to Plastics to Stave Off Losses from Fuel Demand," *DW News*, March 26, 2020, https://www.dw.com/en/plastic-oil-petrochemicals-coronavirus/a-52834661.

The threat and risk to ExxonMobil with this knowledge of its future plans is low. While it is significant that the company is changing the way it utilizes oil that is produced and refined in its facilities, this pivot towards plastic production is not a new or unique approach amongst oil conglomerates and corporations. Indeed, news outlets have reported that many major oil companies have also begun to increase production of plastics to compensate for falling oil demand.[83] A larger concern is that ExxonMobil press releases regarding the modifications to its Baytown, Texas, plant do specify that the company plans to construct its Vistamaxx polymer unit to produce higher grade plastic products.[84] Vistamaxx technology is mostly open source, with technical literature and test methods available for review on Exxon's website; however, online company datasheets specify that the technology does involve the use of a proprietary catalyst technology to produce premium quality plastics.[85] ExxonMobil would incur severe damage if the trade secrets of Vistamaxx's catalyzation process were compromised or stolen. The theft of this technology would lead to a high-risk situation as the misappropriation of this information would nullify any advantage that ExxonMobil has in producing quality plastics for industrial or commercial use and result in potentially significant current and future losses of revenue.

5.2 TAE Technologies

Including their proprietary system—Field Reserved Configuration—in TAE's vacancy announcement poses an informational vulnerability; an adversary can perform targeted research

[83] Beth Gardner, "The Plastics Pipeline: A Surge of New Production Is on the Way," *Yale Environment 360*, December 19, 2019, https://e360.yale.edu/features/the-plastics-pipeline-a-surge-of-new-production-is-on-the-way.

[84] "ExxonMobil's $2 Billion Baytown Chemical Plant Expansion Continues Permian Basin Growth," *Industry Week*, May 2, 2019, https://www.industryweek.com/leadership/companies-executives/article/22027535/exxonmobils-2-billion-baytown-chemical-plant-expansion-continues-permian-basin-growth.

[85] "Product Datasheet: Vistamaxx™ Performance Polymer 8380Propylene Elastomer," *ExxonMobil*, effective July 14, 2020, https://exxonmobilchemical.ulprospector.com/en-US/ds135263/Vistamaxx%E2%84%A2%20Performance%20Polymer%208380.aspx?I=61702&U=1.

on the specified technology. TAE's patent filed with Spanish patent regulators can be found and accessed by performing a simple Internet search using the key phrase "Field Reversed Configuration." Filed in 2018, the published patent provides very detailed specifications of TAE's nuclear fusion reactor and the FRC platform itself. For example, the patent describes the use of both 810 and 820 titanium, coupled with a lithium system that covers the surface of the confinement chamber and the reactor. The patent also includes technical specifications for mirror coils and plasma cannons utilized in the reactor.[86] As previously defined, this patent does protect the information from being reproduced, despite providing detail into TAE's technological process for nuclear fusion. By filing a patent that is now publicly available, TAE has negated any potential confidentiality in exchange for legal protections. However, such legal protections do not prohibit competitors from developing their own systems with knowledge gleaned from patented information.[87]

In addition to its publicly available patent information, TAE Technologies' use of the adjective "proprietary" in its website description of the nuclear fusion technology being developed is an additional vulnerability which could be easily avoided. By describing its FRC system in such a manner on the public webpage, it immediately draws attention from interested parties, serving a signpost that the company is mainly involved in information that would be classified as a trade secret. Furthermore, if a foreign adversary were to conduct web searches using automatic tools programed to collect information containing specific key words, such as

[86] Spanish Patent and Trademark Office, *Method for Forming and Maintaining a High Performance FRC*, patent no. ES 2 658 084 T3 (Madrid, 2018), https://patents.google.com/patent/ES2658084T3/en?q=tae+technologies&inventor=Michl+Binderbauer.
[87] "Industrial Espionage: Cyberattackers Seeking Out Patents," Panda Security, May 8, 2019, https://www.pandasecurity.com/en/mediacenter/security/industrial-espionage-patents-cyberattack/.

"confidential" or "proprietary," TAE's website and associated information could be captured for future analysis and exploitation.

The threat facing TAE as a result of these vulnerabilities is high, as foreign actors have stolen nuclear trade secrets and used patent information to advance development of similar technologies. Online research illustrates that fusion technology is actively being developed by multiple countries around the world, including China. Reports indicate that the Chinese have recently commissioned their indigenous HL-2M fusion reactor in the hopes of producing net energy generation (outputting more energy than is input to initiate the reaction) to facilitate viable commercial fusion technology.[88] China has a history of co-opting insiders to steal nuclear technology. In 2016, the Justice Department prosecuted nuclear engineer Allen Ho and China General Nuclear Power Group with conspiracy to recruit other nuclear engineers to develop and produce special nuclear material in China.[89] The Department of Justice also published a press release asserting that the Chinese People's Liberation Army was involved in widespread theft of trade secrets from U.S. nuclear manufacturer Westinghouse between 2010 and 2011. The military hackers compromised confidential specifications on pipes used within Westinghouse's patented AP1000 reactor to benefit state-owned enterprises.[90]

[88] Caroline Delbert, "China Just Turned on Its Artificial Sun," *Popular Mechanics*, December 4, 2020, https://www.popularmechanics.com/science/energy/a34875771/china-turns-on-artificial-sun-nuclear-fusion-reactor/.

[89] Department of Justice, Office of Public Affairs, "U.S. Nuclear Engineer, China General Nuclear Power Company and Energy Technology International Indicted in Nuclear Power Conspiracy against the United States," press release, April 16, 2019, https://www.justice.gov/opa/pr/us-nuclear-engineer-china-general-nuclear-power-company-and-energy-technology-international.

[90] Department of Justice, Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," press release, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

TAE faces a higher risk to its business, given that its proprietary technology is highlighted by the company in its online materials—either as a matter of pride or as sense of accomplishment. TAE's website's emphasis on the adjective "proprietary" draws undue attention from users, including foreign adversaries. In using Internet search engines to connect "TAE Technologies" and "proprietary" or "Field Reversed Configuration," the company's online Spanish patent for the technology becomes readily accessible to anyone. TAE is faced with a real risk of information compromise that could allow a malicious actor to develop technology like FRC, as exemplified in the recent attempts made by China to steal nuclear trade secrets and its aggressive development of nuclear fusion technology. The company has rested its future existence, and nuclear power market advantage, on the successful development and production of the novel FRC fusion system. Production of systems similar to the FRC, using data from the Spanish patent, could single-handedly upend TAE's business model as the developer of a unique approach to fusion; this could pose an existential threat to its business.

5.3 Pfizer

Similarly, Pfizer's job posting requesting an applicant to have oncology and hemophilia contracting experience could present an information vulnerability. This job vacancy requirement helps to showcase the company's attempts to create new, future revenue sources. The push to launch new cures for hemophilia represents a metaphoric insurance policy for Pfizer, as it faces expirations on its patents later in the decade. Online news sources specify that upwards of $20 billion in Pfizer patents are set to expire by 2030, leading to a major loss in revenue for the company. The public announcements of new drugs and continuations of trial studies potentially represents the company's preemptive attempts to create new revenue streams to make up for the

loss in profit.[91] Oncology products also form an integral part of Pfizer's future strategy to boost revenues. Open-source research details that the company is positioning oncology, along with hemophilia, as a main pillar of its future development, with a forecasted $6 billion increase in oncology-related products by 2027.[92]

As Pfizer's competition with BioMarin to enter phase 3 hemophilia drug trials illustrates, the healthcare (pharmaceutical) industry can be a cutthroat business, with large amounts of money at stake. While Pfizer has openly discussed its developments of both hemophilia and oncological drugs, it has not detailed its future business plans. Pfizer's standing in the global drug marketplace rests upon maintaining a regulatory advantage regarding new cures for these two diseases. The threat to Pfizer from this vacancy announcement is moderate. The company has been open about its new hemophilia and oncology drugs; other companies are aware, and are racing to develop their own medicines. Nevertheless, foreign actors have recently targeted U.S. drugmakers to steal vital research and development data. The BBC reported that, in 2020, two Chinese men were charged with corporate espionage after hacking biotechnology companies in Maryland and Massachusetts. The targeted companies were researching coronavirus vaccines and treatments. The men allegedly had the support of China's Ministry of State Security.[93] Despite the moderate threat, the overall risk to Pfizer is high, given that much of the company's future revenue goals depend on being one of the first businesses to market innovative cures for hemophilia and cancer. These cures were supposed to make up for expected lost revenue from

[91] Nick Paul Taylor, "Roche Targets 2021 Start for Hemophilia A Gene Therapy Phase 3 as Optimization Effort Drags On," *Fierce Biotech*, July, 13 2020, https://www.fiercebiotech.com/biotech/roche-targets-2021-start-for-hemophilia-a-gene-therapy-phase-3-as-optimization-effort-drags.
[92] Jessica Merrill, "Pfizer Oncology Pipeline Shows Pivot to Targeted Therapies," *Scrip Informa Pharma Intelligence*, September 22, 2020, https://scrip.pharmaintelligence.informa.com/SC143001/Pfizer-Oncology-Pipeline-Shows-Pivot-To-Targeted-Therapies.
[93] "US Charge Chinese COVID-19 Research 'Cyber Spies,'" *BBC*, July 21, 2020, https://www.bbc.com/news/world-us-canada-53493028.

patent expirations, and if such expectations are not achieved, the company could experience significant losses in revenue. Pfizer's current drug research and development is most likely highly sought after by foreign drugmakers, both allies and adversaries.

5.4 HCA Healthcare

HCA Healthcare's announcement, which advertises the company's reliance on Azure AD to perform identity and access management, presents an informational vulnerability to the company, if Azure AD is not continually monitored, patched, and secured. According to online reporting, Azure AD has been subjected to known exploitation as recently as 2020. If an Azure account with a weak password can be compromised, an attacker can gain a foothold in an internal network and use computer tools to decrypt additional user passwords and administrator accounts. News sources indicate that the COVID-19 pandemic, and the subsequent rapid transition to telework, has left many Azure AD systems with configuration errors that can allow anyone to access a company's virtual network. Additionally, COVID-19 has made Azure AD more permissive of external users and third-party applications given the need to telework, allowing external applications the ability to access company data.[94]

HCA's job posting's advertised use of Microsoft programs is not limited to Azure AD, but also includes Microsoft's SQL Server, which has been subjected to recent intrusions. On its website, Microsoft describes SQL Server as a database management system.[95] News sources detail that SQL Server has experienced long-running attacks against it, dating to 2017. These

[94] Ben Dickson, "Cloud Security: Attacking Azure AD to Expose Sensitive Accounts and Assets," *The Daily Swig*, May 14, 2020, https://portswigger.net/daily-swig/cloud-security-attacking-azure-ad-to-expose-sensitive-accounts-and-assets.

[95] "SQL Server 2019," Microsoft, accessed June 4, 2021, https://www.microsoft.com/en-us/sql-server/sql-server-2019.

attacks use forced passwords to breach servers, deploying backdoor access that allow malicious data mining tools to continuously gather information. In total, 3,000 SQL servers have been affected, including those used by healthcare companies based in the United States.[96]

SQL Server's vulnerabilities are shared by JavaScript, the other technical application mentioned in the HCA announcement, which may be used to create internal websites. JavaScript is described as the "language" of the Internet. Information technology publications state that it is used to update websites tailored to customers' needs. Embedded within each webpage is JavaScript coding, with nearly half of all websites utilizing the programming. Industry sources contend that JavaScript itself has numerous vulnerabilities, most significantly the ability of an actor to embed malicious code into a webpage that can track content, log keystrokes, and archive browser cookies. After logging these three pieces of data, forming a digital picture of a user's habits, a hacker can embed bad code into a webpage to steal data and access security permissions to compromise additional webpages.[97]

HCA's job announcement, advertising the use of Microsoft Azure AD, SQL Server, and JavaScript create a high threat of compromise to the company, as these systems and applications have historically been penetrated by foreign intelligence entities and contain unresolved weaknesses. Since December 2020, the Department of Homeland Security (DHS) assessed that the Russian Foreign Intelligence Service (SVR) has successfully penetrated Microsoft Cloud, including Azure AD, after accessing networks. The SVR uses this access to steal information and

[96] Ohpir Harpaz, "The Vollgar Campaign: MS-SQL Servers Under Attack," *GuardianCore*, accessed June 4, 2021, https://www.guardicore.com/blog/vollgar-ms-sql-servers-under-attack/.
[97] Ebubekir Buber, "How Companies Are Hacked via Malicious JavaScript Code," *ITNEXT*, February 15, 2019, https://itnext.io/how-companies-are-hacked-via-malicious-javascript-code-12aa82560bdc.

create backdoors to maintain access.[98] DHS reports that foreign intelligence has also exploited vulnerabilities within Azure AD to generate additional user authentication credentials that appear legitimate, allowing consistent access to internal systems, without arousing undue suspicion.[99] The National Institute for Standards and Technology (NIST) is currently tracking two main vulnerabilities for Azure AD - sign-in bypass and active identity spoofing - to circumvent authentication requirements. NIST has designated these vulnerabilities as critical and medium threats, respectively.[100] NIST is also tracking 50 ongoing issues with SQL Server from February to May 2021.[101]

The vulnerabilities of Microsoft Azure AD, SQL Server, and JavaScript, together with the threats from foreign intelligence agencies, facilitate a high-risk environment for HCA Healthcare. If its identity and access management system is compromised, the risks posed to HCA's internal network are extraordinary. The current issues affecting Azure AD, the vendor-provided platform HCA's access management tools run on, are compounded by the ongoing interest in the Microsoft system from foreign intelligence. The nature of HCA Healthcare's information stored on its networks—which may include PII, patient lists, vendors, cost sheets—and the ability of an actor to compromise the Azure AD platform to gain unauthorized access, which can then catalyze further breaches of the network's SQL servers, creates a risk that, if

[98] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise*, May 14, 2021, https://us-cert.cisa.gov/remediating-apt-compromised-networks.

[99] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, alert AA20-352A, revised April 15, 2021, https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[100] U.S. Department of Commerce, National Institute for Standards and Technology, "National Vulnerability Database: CVE-2021-2702," accessed June 4, 2021.

[101] U.S. Department of Commerce, National Institute for Standards and Technology, "National Vulnerability Database: SQL Server," accessed June 4, 2021.

found and exploited, can compromise the company's entire network and halt operations for an extended period.

5.5 Pratt and Whitney

Much like the cybersecurity risks facing HCA Healthcare's identity and access management platform, Pratt and Whitney's job announcement's disclosure of the use of Lenel's OnGuard integrated security system poses an informational and organizational vulnerability. Lenel's website's open declaration of the partners it collaborates with to develop the OnGuard system could be used to target the supply chains of these partner companies to compromise the physical security systems within P&W's headquarters. News sources explain that access control systems connected to the Internet, which OnGuard can be,[102] increases vulnerability to the system. Network connection of a physical security system to remotely control alarms, cameras, and locks opens another entry point for hackers looking to gain broader network access. If malign actors can gain unauthorized network access through the physical security system, they can unlock doors or take security sensors offline.[103]

With the potential of the OnGuard system to be bypassed, the threat to P&W's headquarters campus is high, especially considering a recent physical security failure at Google, combined with the 2015 publication of P&W's campus map online. The incident at Google was not malicious but exhibited the ability of a cyber attacker to defeat physical security systems. Open-source research detailed that in 2017, a Google engineer at the company's Sunnyvale,

[102] "OnGuard Access Sheet," Lenel, accessed June 23, 2021, https://www.lenel.com/assets/library/onguard/OG_SS_AC_new%20format.pdf.
[103] Megan Gates, "Assessing Cyber Risks to Your Access Control Systems," *ASIS Online*, March 1, 2020, https://www.asisonline.org/security-management-magazine/articles/2020/03/assessing-cyber-risks-to-your-access-control-system/.

California, campus used malicious code to forge encryption commands used by a third-party vendor. Using this fake material, the engineer was able to fool radio-frequency identification (RFID) card readers into opening doors and locking others.[104] In addition to risks presented by cyberattacks, another major threat to physical security at the P&W campus comes from the publication of campus maps online.

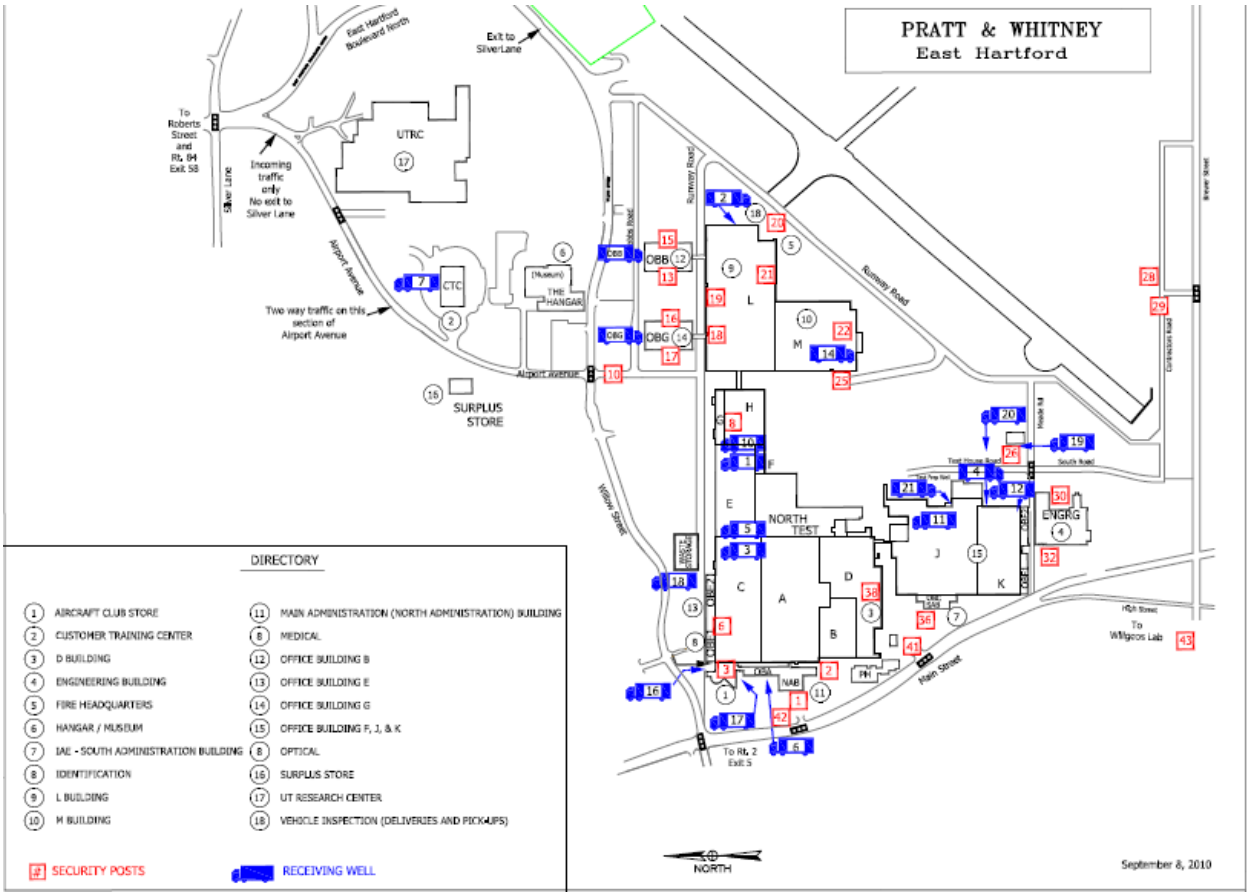

Figure 5.5. Pratt and Whitney's Campus Map in East Hartford, Connecticut. (Map downloaded from the NASA-Connecticut Space Grant Consortium, *Pratt & Whitney, East Hartford*, July 2015, Connecticut Space Grant Consortium, https://ctspacegrant.org/wp-content/uploads/2015/07/Map-of-PW-Museum-Hangar-parking.pdf)

[104] Thomas Brewster, "Google's Doors Hacked Wide Open by Own Employee," *Forbes*, September 3, 2018, https://www.forbes.com/sites/thomasbrewster/2018/09/03/googles-doors-hacked-wide-open-by-own-employee/?sh=6a7719ac3c7a.

Figure 5.5 displays a representation of the company's headquarters campus (as it appeared in 2010), listing access roads, specific buildings, security checkpoints, and locations for receiving cargo by truck. Relevant to this discussion is the map's display of the 26 security posts scattered throughout the campus.[105] These security checkpoints illustrated in the visualization can be used by bad actors, along with the knowledge of the Lenel OnGuard system, to map out locations with, or without, a security checkpoint. Knowledge of security checkpoints, in conjunction with cyber exploitation of the OnGuard system to take specific physical security components at certain locations offline, can be used to conduct human-sourced infiltration of the campus. This infiltration may not necessarily have the goal of espionage or theft of information, but could also include violent extremists looking to attack a U.S. corporate entity. The risk to P&W is ranked as moderate given the high threat potential but multiple unknowns surrounding the company's use of Lenel and the current physical security situation at headquarters, which could negate threats posed by the 2010 campus map. As mentioned, the greatest vulnerability to Lenel's security apparatus is its internet connection. It is unknown how P&W has set up its OnGuard system in terms of connectivity—a local area network limited to the campus or a wider network extending into the surrounding area—and the level of protection the company has provided to the system through firewalls, VPN, or 24/7 monitoring. Furthermore, if the system were only connected to a local area network—company intranet—the Google incident proves that an insider threat could still compromise the system. Additionally, since maps can become outdated with physical

[105] NASA-Connecticut Space Grant Consortium, *Pratt & Whitney, East Hartford*, July 2015, map, Connecticut Space Grant Consortium, https://ctspacegrant.org/wp-content/uploads/2015/07/Map-of-PW-Museum-Hangar-parking.pdf).

changes and security posts can change locations in response to needs, using the 2010 map may not be a reliable means to plan a physical penetration.

5.6 Spinlaunch

The vulnerabilities to start-up rocketry firm Spinlaunch are less severe. While Spinlaunch's job announcement makes clear that Spinlaunch seeks to develop small satellite buses to compete in the imagery or broadband network business, it is likely doing so out of necessity; current conventional satellite systems cannot withstand the extreme centrifugal launch forces created by the company's unique platform. Internet searches indicate that Spinlaunch appears to be the only space company marketing such a launch service.

Despite the vulnerability, the threat to the Spinlaunch is moderate. The main threat to the company may occur during the design phase of any satellite buses to be used on its rocket. These standardized buses would be hardened and reinforced to withstand the dynamic physical forces exerted on them during ascent. Spinlaunch may face future threats from adversary nations, notably China and Russia, who have sought to acquire U.S. technologies for military modernization. In this context, any technology developed by Spinlaunch would be of interest for foreign nations developing innovative components for use in adverse environments. News sources detail that such an event occurred in 2019, when an interlocuter working for Chinese aerospace companies was arrested by the FBI for attempting to smuggle radiation-resistant microchips into China. These microchips could be used in military satellites.[106]

[106] Justin Rohrlich and Tim Fernholz, "China is Trying to Steal Military Space Tech. The US is Running Stings to Stop it," *Quartz*, September 16, 2019, https://qz.com/1702414/inside-the-fight-to-keep-us-military-space-tech-out-of-china/.

The risk to the company is moderate, given the previously mentioned proclivity of foreign adversaries and allies to steal U.S. corporate trade secrets to benefit homegrown industry and defense, but tempered by the fact that, presently, no thefts of hardened satellite buses or unique launch systems have been made public. If theft of Spinlaunch's satellite design does occur, the company's business strategy would be put in jeopardy, since it relies on the innovative centrifugal launch platform and its own satellite technology to attract customers seeking a new way to reach orbit.

5.7 Statistical Results

With the above analysis of vulnerabilities, threats, and risks, is the proposed hypothesis validated? No. While the vacancy announcements do present some instances of information and organizational vulnerabilities, they represent a tiny fraction of the job postings that are currently on the Internet. Out of the seventy job posts reviewed for this project, only six were identified as having any potentially problematic data within, totaling only 8.5%. Thus, the issue is not necessarily pervasive. This number is much less than the 50% needed to justify the hypothesis. Concerning the three types of the variables analyzed within job listings—informational, organizational, and personnel—all six cases displayed information vulnerabilities and two disclosed an organizational vulnerability in concert with informational vulnerability—ExxonMobil and Pratt and Whitney. No vacancies reviewed provided personal contact information for hiring officials, with companies relying on general email addresses or phone numbers for their human resources departments.

Table 5.7. Summarized Case Study Vulnerabilities (Table by Author).

Industry	Job Title	Vulnerabilities
Energy	ExxonMobil / “HR Senior Manufacturing Professional"	Correlation of the concept of change management with facility upgrades at the vacancies’ job locations--Baytown, Baton Rouge, and Beaumont-- illustrates Exxon's future, nonpublic, strategic pivot towards plastics production.
Energy	TAE Technologies / "Scientist—Modeling Stability and Fast Ion Physics"	Proprietary Field Reversed Configuration (FRC) system, published by Spanish patent office, providing comprehensive information on FRC configuration and components.
Healthcare	Pfizer / "Senior Associate, Contracting Management"	Company's need for experience in hemophilia and oncology contracting experience indicates its future plans to develop and manufacture new treatments for these two diseases, resting much of its future revenue on these cures.
Healthcare	HCA Healthcare / “Identity and Access Management Security Developer”	Vacancy discloses system vendor information, Microsoft, supporting the company’s identity management software (Azure AD) and internal websites (JavaScript and SQL Server). All three applications have critical, ongoing vulnerabilities that can be used to penetrate networks.
Aviation	Spinlaunch / "Senior Satellite Systems Engineer"	Job listing divulges the need for a small satellite bus as no current conventional satellite systems have been designed for such extreme launch conditions. The company faces a significant threat and risk during the design phase of any future satellite platform as foreign countries would be interested in obtaining data that could assist in the development of future military technologies.
Aviation	Pratt and Whitney / "Global Security Technology Manager"	The job post’s details HQ address and the physical security vendor, Lenel. Lenel's disclosure of the partner companies it collaborates with to develop the OnGuard Enterprise system can facilitate easy targeting of component supply chains—locks, cameras, or biometric readers.

5.8 What if the Hypothesis was Validated?

If the hypothesis was validated, there are multiple policy prescriptions that could be implemented to reduce the vulnerabilities and risks presented by vacancy announcements. One would be the creation of common security requirements for handling and storing sensitive and

non-sensitive information held by U.S. businesses. Such standards already exist within federal agencies, protecting both classified and unclassified information, but do not apply to private industry. These requirements would perhaps take the form of standardized information security, physical security, and personnel security policies that companies must administer to mitigate potential vulnerabilities and reduce risk. Equitable, rather than equal, treatment of companies—both large and small—would be the main challenge of any such standardized regulations. For instance, would it be fair to ask start-up TAE Technologies to implement the same complex security measures as ExxonMobil? Public-private collaborative opportunities should also be utilized to address the risks of non-sensitive information. The Office of the Director of National Intelligence currently maintains multiple cooperative programs with private industry to provide threat briefings and incident response, among other activities.[107] This collaboration should be expanded to analyze the threats posed by the ever-increasing quantities of non-sensitive information, including job listings. Such an approach would broaden the security mindset of companies to ponder the public dissemination of detailed non-sensitive information.

5.9 Limitations of the Research Study

This analysis may not directly benefit the existing literature, as it does not delve into discussing how these affected companies protect their trade secrets, apart from HCA's and P&W's use of information security and physical security systems. However, this project can contribute to the literature by describing the potential threats posed by non-sensitive information in the pre-hire process, spawning a new set of academics and thinkers to wholistically analyze many more vacancies, potentially hundreds more than what have been analyzed here.

[107] "National Security Partnerships," U.S. Office of the Director of National Intelligence, accessed August 3, 2021, https://www.dni.gov/index.php/ncsc-how-we-work/314-about/organization/national-security-partnerships.

Furthermore, given the relatively small sample size—seventy posts—the conclusions reached regarding vulnerabilities, threats, and risks may be disproven with a broader analytical approach. Likewise, with a larger sample, the number of job listings with potentially risky information may also grow, highlighting a more significant problem with vacancy announcements than has been illustrated in this study.

6. Conclusion

Over the past twenty years, globalization has spurred companies to become global themselves, taking advantage of technology to increase their worldwide profits. The Internet has played an outsized role in the development of modern companies; likewise, the Internet serves as most companies' main gateway for recruiting new talent. With tens of thousands of job listings currently advertised by private companies within the United States, the information contained within such listings is accessible to anyone around the world with a computer. How do vacancy announcements pose security risks and vulnerabilities to U.S. private organizations? Analysis of six companies studied across three industries illustrates that job postings present informational and organizational vulnerabilities to companies, with none posing risks to personnel. It is estimated, based upon the study samples, that a small minority of vacancies contain potentially damaging information. Are there any practical implications of this research? The most important implication of this study is that vacancy announcements, rather than being seen as mundane, everyday work processes to be completed by HR departments, should be seen as potential sources of vulnerability and compromise. Information presented in the announcements should be carefully vetted. Another important conclusion is that non-sensitive information, contained in such announcements, can be used with malicious intent; it can be compiled, collated, and analyzed to reveal company trade secrets. This is not to say that all job listings currently

advertised online need to be taken down and reviewed, but rather, companies should adjust their information security processes to account for the risks inherent in releasing detailed job information to the public. In the current technological age, security risks can come from any actor, across multiple platforms, using data that is online. Adversarial actors can, and will, continue to steal trade secrets using multiple avenues of exploitation. Vacancy announcements provide an additional mechanism that bad actors can use to gain knowledge and information to formulate a targeting profile of a company. Private industry needs to be cognizant of the information they release to the public and be more aware of the dynamic security threat environment and the evolving methods foreign actors use to penetrate and exfiltrate information.

Bibliography

Vacancy Announcements

"Global Security Technology Manager." *Pratt and Whitney.* Posted May 12, 2021. https://jobs.prattwhitney.com/job/east-hartford/global-security-technology-manager/1737/19369400

"HR Senior Manufacturing Professional." *ExxonMobil*. Posted May 21, 2021. https://jobs.exxonmobil.com/ExxonMobil/job/Houston-HR-Senior-Manufacturing-Professional-TX-77001/747277300/.

"Identity and Access Management Security Developer." HCA Healthcare. Accessed June 3, 2021. Identity and Access Management Security Developer in Nashville, Tennessee, United States (hcahealthcare.com).

"Scientist—Modeling Stability and Fast Ion Physics." *TAE Technologies*. Posted May 17, 2021. https://recruiting2.ultipro.com/TRI1021TRIAE/JobBoard/49386e5d-f909-4648-8335-415ce97e3f15/OpportunityDetail?opportunityId=46f59c3f-f100-4a6a-9316-28fed59b9253.

"Senior Associate, Contracting Management." *Pfizer*. Posted June 1, 2021. https://pfizer.wd1.myworkdayjobs.com/en-US/PfizerCareers/job/United-States---Illinois---Lake-Forest/Senior-Associate--Contract-Management_4814121.

"Senior Satellite Systems Engineer." Spinlaunch. Accessed June 11, 2021. https://www.google.com/search?client=firefox-b-1-d&q=spinlaunch+jobs&ibp=htl;jobs&sa=X&ved=2ahUKEwjsjumPs4nxAhXbF1kFHZ1OBaIQudcGKAJ6BAgDEC4#htivrt=jobs&htidocid=LdYllHflkxd-odkSAAAAAA%3D%3D&fpstate=tldetail.

Corporate Resources

"Azure Active Directory." Microsoft. Accessed June 4, 2021. https://azure.microsoft.com/en-us/services/active-directory/.

"Contact Us." Pratt and Whitney. Accessed June 18, 2021. https://prattwhitney.com/company/contact-us.

"Frequently Asked Questions." TAE Technologies. Accessed June 5, 2021. https://tae.com/about-us/faq/.

"Growing the Gulf." ExxonMobil. Accessed June 1, 2021. https://corporate.exxonmobil.com/Locations/United-States/Growing-the-Gulf.

"Integrated Security Management Software." Lenel. Last updated 2015. https://www.lenel.com/assets/library/onguard/OG_SS_ENT_0515_new%20format.pdf.

"OAAP Partners and Products." Lenel. Accessed June 10, 2021. https://www.lenel.com/solutions/open-integration/oaap/partners-products-search.

"OnGuard Access Sheet." Lenel. Accessed June 23, 2021, https://www.lenel.com/assets/library/onguard/OG_SS_AC_new%20format.pdf.

"Product Datasheet: Vistamaxx™ Performance Polymer 8380Propylene Elastomer." *ExxonMobil*. Effective July 14, 2020. https://exxonmobilchemical.ulprospector.com/en-US/ds135263/Vistamaxx%E2%84%A2%20Performance%20Polymer%208380.aspx?I=61702&U=1.

"PW Unveils New Engineering and Technology Center on its East Hartford Campus." *Pratt and Whitney*. November 11, 2017. https://newsroom.prattwhitney.com/2017-11-11-Pratt-Whitney-Unveils-New-Engineering-and-Technology-Center-on-its-East-Hartford-Campus.

"SQL Server 2019." Microsoft. Accessed June 4, 2021. https://www.microsoft.com/en-us/sql-server/sql-server-2019.

Scholarly Articles and Books

Androulidakis, Iosif, and Fragkiskos – Emmanouil Kioupakis. *Industrial Espionage and Technical Surveillance Counter Measures.* Switzerland: Springer International, 2016. https://www.springer.com/gp/book/9783319286655.

Bahrudin, I.S., B. Abdullah, N.A. Mohd Sallh, and P. Shariffudin. "A Case Study on Change Management Readiness for an Oil & Gas SME Company in Malaysia." Presented at the 6th *International Conference on Advances in Mechanical Engineering*, *Kota Kinabalu, Sabah, Malaysia, August 14-16, 2019*.

Chitalutu, Premkumar, and Ravi Prakash. "Organizational Security Policies and Their After Effects." In *Information Security and Optimization*, edited by Rohit Tanwar, Tanupriya Choudhury, Mazdak Zamani, and Sunil Gupta, 43-60. Baton Rouge, LA: CRC Press, 2020. https://www.taylorfrancis.com/books/edit/10.1201/9781003045854/information-security-optimization-rohit-tanwar-tanupriya-choudhury-mazdak-zamani-sunil-gupta.

Epstein, Richard. "The Constitutional Protection of Trade Secrets Under the Takings Clause." *University of Chicago Law Review* 57, (2004): 57-75. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2200&context=journal_articles.

European Union's Institute for Security Studies. *The Threat of State-Sponsored Industrial Espionage*, by Massimo Pellegrino. Paris, France, 2015. https://www.iss.europa.eu/content/threat-state-sponsored-industrial-espionage.

Gabric, Marko. "Incorporating Security Elements." *In Corporate Security Management, Challenges, Risks, and Strategies*. Oxford, UK: Butterworth Heinemann, 2015.

Koen, Clifford, Jr., and Brian London. "To Catch a Thief: Protecting Proprietary Information Including Trade Secrets From Corporate Espionage." *Health Care Manager* 38, no.4 (2008): 331-342. https://pubmed.ncbi.nlm.nih.gov/31663872/.

Reid, Melanie. "A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? Effectively Dealing With This Global Threat?" *University of Miami Law Review* 70 (2016): 756-829. https://repository.law.miami.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4468&context=umlr.

Richmond, Rick, and Sandra Hanian. "Protecting Trade Secrets in Government Contracting." In *Government Contracting Law Report* 4, no.3, 72-76. New York: LexisNexus, 2018. https://jenner.com/system/assets/publications/17827/original/Rick%20Richmond%20and%20Sandra%20Hanian.pdf?1520963384.

Scott, Craig. *Anonymous Agencies, Backstreet Businesses, and Covert Collectives: Rethinking Organizations in the 21st Century.* Stanford: Stanford University Press, 2018.

Sengar, D.S. "Protection of Trade Secrets and Undisclosed Information: Law and Litigation." *Journal of the Indian Law Institute* 2, no.53 (2011): 254-274. https://www.jstor.org/stable/43953505.

Government Publications

Food Marketing Institute v. Argus Leader Media. 588 U.S. 1 (2019).

"National Security Partnerships." U.S. Office of the Director of National Intelligence. Accessed August 3, 2021. https://www.dni.gov/index.php/ncsc-how-we-work/314-about/organization/national-security-partnerships.

"Trade Secrets Policy." *U.S. Patent and Trademark Office*. February 7, 2019. https://www.uspto.gov/ip-policy/trade-secret-policy.

U.S. Congressional Research Service. *Protection of Trade Secrets: Overview of Current Law and Legislation*, by Brian Yen. Report R43714. Washington, DC, 2016. https://fas.org/sgp/crs/secrecy/R43714.pdf.

U.S. Department of Commerce, National Institute for Standards and Technology. *Guide for Conducting Risk Assessments: Information Security.* September, 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

_____. "National Vulnerability Database: CVE-2021-2702." Accessed June 4, 2021.

_____. "National Vulnerability Database: SQL Server." Accessed June 4, 2021.

U.S. Defense Counterintelligence and Security Agency. *Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry.* December 2020. https://www.dcsa.mil/Portals/91/Documents/CI/2020-Targeting-US-Technologies_Briefing.pdf.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations.* Alert AA20-352A. Revised April 15, 2021, https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

_____. *Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise.* May 14, 2021. https://us-cert.cisa.gov/remediating-apt-compromised-networks.

U.S. Department of Justice, Office of Public Affairs. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." Press Release. March 23, 2018. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

_____. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Press Release. May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

U.S. Environmental Protection Agency. *Plastics: Material-Specific Data*. Accessed June 10, 2021, https://www.epa.gov/facts-and-figures-about-materials-waste-and-recycling/plastics-material-specific-data.

U.S. Merit Systems Protection Board. *Help Wanted: A Review of Federal Vacancy Announcements.* April, 2003. https://www.mspb.gov/MSPBSEARCH/viewdocs.aspx?docnumber=253634&version=1831327&application=ACROBAT.

U.S. National Aeronautics and Space Administration. *Information Technology Threats and Vulnerabilities*. Accessed June 10, 2021. https://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm.

U.S. Office of the Director of National Intelligence. National Counterintelligence and Security Center. *Foreign Economic Espionage in Cyberspace.* July, 2018. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

_____. *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011. October, 2011.* https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

_____. *National Counterintelligence Strategy of the United States of America 2020-2022.* February, 2020. https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

U.S. Patent and Trademark Office. *Trade Secret Protection in the United States*. https://www.nist.gov/system/files/documents/mep/marinaslides.pdf.

Spanish Patent and Trademark Office. *Method for Forming and Maintaining a High Performance FRC*. Patent number ES 2 658 084 T3. Madrid, 2018. https://patents.google.com/patent/ES2658084T3/en?q=tae+technologies&inventor=Michl+Binderbauer.

News Reports

Alpert, Bill. "How Pfizer Plans to Lead the Industry in Gene Therapies." *Barron's*. September, 16, 2020. https://www.barrons.com/articles/how-pfizer-plans-to-lead-the-industry-in-gene-therapies-51600197117.

Brelsford, Robert. "ExxonMobil Commissions Beaumont Polyethylene Expansion." *Oil and Gas Journal*. February 25, 2019. https://www.ogj.com/refining-processing/petrochemicals/article/14036785/exxonmobil-commissions-beaumont-polyethylene-expansion.

Brewster, Thomas. "Google's Doors Hacked Wide Open by Own Employee." *Forbes*. September 3, 2018. https://www.forbes.com/sites/thomasbrewster/2018/09/03/googles-doors-hacked-wide-open-by-own-employee/?sh=6a7719ac3c7a.

Buber, Ebubekir. "How Companies Are Hacked via Malicious JavaScript Code." *ITNEXT*. February 15, 2019. https://itnext.io/how-companies-are-hacked-via-malicious-javascript-code-12aa82560bdc.

Dickson, Ben. "Cloud Security: Attacking Azure AD to Expose Sensitive Accounts and Assets." *The Daily Swig*. May 14, 2020. https://portswigger.net/daily-swig/cloud-security-attacking-azure-ad-to-expose-sensitive-accounts-and-assets.

Ewing, Philip. "Gates: French Cyber Spies Target U.S." *Politico*. May 22, 2014. https://www.politico.com/story/2014/05/france-intellectual-property-theft-107020.

"Explaining the Defend Trade Secrets Act." *American Bar Association*. September 9, 2016. https://www.americanbar.org/groups/business_law/publications/blt/2016/09/03_cohen/.

"ExxonMobil's $2 Billion Baytown Chemical Plant Expansion Continues Permian Basin Growth." *Industry Week.* May 2, 2019. https://www.industryweek.com/leadership/companies-executives/article/22027535/exxonmobils-2-billion-baytown-chemical-plant-expansion-continues-permian-basin-growth.

Fruhlinger, Josh. "What is Corporate Espionage? Inside the Murkey World of Private Spying." *CSO Online*. July 2, 2018. https://www.csoonline.com/article/3285726/what-is-corporate-espionage-inside-the-murky-world-of-private-spying.html.

Gardner, Beth. "The Plastics Pipeline: A Surge of New Production Is on the Way." *Yale Environment 360*. December 19, 2019. https://e360.yale.edu/features/the-plastics-pipeline-a-surge-of-new-production-is-on-the-way.

Gardner, Jonathan. "Pfizer Lays Out Gene Therapy Aspirations." *BioPharma Drive*. January, 28, 2020. https://www.biopharmadive.com/news/pfizer-gene-therapy-phase-3-dmd-hemophilia/571238/.

Gates, Megan. "Assessing Cyber Risks to Your Access Control Systems." *ASIS Online*. March 1, 2020. https://www.asisonline.org/security-management-magazine/articles/2020/03/assessing-cyber-risks-to-your-access-control-system/.

Harpaz, Ohpir. "The Vollgar Campaign: MS-SQL Servers Under Attack." *GuardianCore*. Accessed June 4, 2021. https://www.guardicore.com/blog/vollgar-ms-sql-servers-under-attack/.

Hunter, Caroline. "U.S. FDA Rejects BioMarin Hemophilia Gene Therapy, Shares Dive." *Reuters*. August, 19, 2020. https://www.reuters.com/article/us-biomarin-pharma-fda/u-s-fda-rejects-biomarin-hemophilia-a-gene-therapy-shares-dive-idUSKCN25F1H6.

Laskai, Lorrand, and Adam Segal. "A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage." *Council on Foreign Relations*. December 2018. https://www.cfr.org/report/threat-chinese-espionage.

Masbrucker, Kristen. "ExxonMobil Mulls $334 Million Chemical Facility Expansion in Baton Rouge, Seeks Incentives." *Advocate* (Baton Rouge, LA), March 30, 2021. https://www.theadvocate.com/baton_rouge/news/business/article_9aa51b6e-9176-11eb-a0e3-1f5b6c15f4e9.html.

Merrill, Jessica. "Pfizer Oncology Pipeline Shows Pivot to Targeted Therapies." *Scrip Informa Pharma Intelligence*. September 22, 2020. https://scrip.pharmaintelligence.informa.com/SC143001/Pfizer-Oncology-Pipeline-Shows-Pivot-To-Targeted-Therapies.

NASA-Connecticut Space Grant Consortium. *Pratt & Whitney, East Hartford*. July 2015. Map. Connecticut Space Grant Consortium. https://ctspacegrant.org/wp-content/uploads/2015/07/Map-of-PW-Museum-Hangar-parking.pdf.

Niranjan, Ajit. "Oil Companies Pivot to Plastics to Stave Off Losses from Fuel Demand." *DW News*. March 26, 2020. https://www.dw.com/en/plastic-oil-petrochemicals-coronavirus/a-52834661.

Oberhaus, Daniel. "Inside Spinlaunch, the Space Industry's Best Kept Secret." *Wired*. January 29, 2020. https://www.wired.com/story/inside-spinlaunch-the-space-industrys-best-kept-secret/

"Pfizer, Sangamo dose first participant in phase 3 study of Hemophilia A gene therapy treatment." *Pharmaceutical Business Review*. October 8, 2020. https://www.pharmaceutical-business-review.com/news/pfizer-sangamo-dose-first-participant-in-phase-3-study-of-hemophilia-a-gene-therapy-treatment/.

Priestap, Bill, and Holden Triplett. "The Espionage Threat to U.S. Business." *Lawfare*. October 10, 2020. https://www.lawfareblog.com/espionage-threat-us-businesses.

Rohrlich, Justin, and Tim Fernholz. "China is Trying to Steal Military Space Tech. The US is Running Stings to Stop it." *Quartz*. September 16, 2019. https://qz.com/1702414/inside-the-fight-to-keep-us-military-space-tech-out-of-china/.

Shane, Daniel. "How China gets what it wants from American Companies." *CNN Money*. April 5, 2018. https://money.cnn.com/2018/04/05/news/economy/china-foreign-companies-restrictions/index.html.

Taylor, Nick Paul. "Roche Targets 2021 Start for Hemophilia A Gene Therapy Phase 3 as Optimization Effort Drags On." *Fierce Biotech*. July, 13 2020. https://www.fiercebiotech.com/biotech/roche-targets-2021-start-for-hemophilia-a-gene-therapy-phase-3-as-optimization-effort-drags.

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

"Upcoming Potential Advances in the Treatment of Hemophilia." *Ascella Health*. June 2020. https://www.ascellahealth.com/sites/default/files/files/document/june_2020_-_advances_in_hemophilia_treatment.pdf.

"US Charge Chinese COVID-19 Research 'Cyber Spies.'" *BBC*. July 21,2020. https://www.bbc.com/news/world-us-canada-53493028.

"What is Identity and Access Management." Cloudflare. Accessed June 4, 2021. https://www.cloudflare.com/learning/access-management/what-is-identity-and-access-management/.

Wong, Edward. "How China Uses LinkedIn to Recruit Spies Abroad." *New York Times*. September 27, 2019. https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.

Curriculum Vitae

Drew Mesa was born in Washington, D.C., on September 11, 1995. He pursued his undergraduate studies at the University of Mary Washington (UMW) in Fredericksburg, Virginia. He graduated from UMW in May 2018, *magna cum laude* with departmental honors, with a Bachelor's of Arts degree in History with a minor in Security and Conflict Studies. Since graduating, he has held positions at the Food and Drug Administration and the Transportation Security Administration, as a program analyst and personnel security specialist, respectively.