Global Information Assurance Certification Paper

Information Security Starts with the Employees

GIAC (GSLC) Gold Certification

Author: Simone (Cy) Genna, cy@cyber-cy.com
Advisor: *Jonathan Risto*

Accepted: *May 31, 2021*

Abstract

Organizations continue to spend exorbitant budgets to combat the issue of insider threat with one source estimating it at $270B/year by 2026 (Forbes, 2020). By comparison, the cost to put a man on the moon, possibly the greatest accomplishment in the history of mankind, was $283B (adjusted for inflation) and that was spread across thirteen years from 1960 to 1973. The cybersecurity industry's approach to insiders has reached a tipping point where the methodology and framework have become unscalable, inefficient, and ineffective. The only strategy appears to be doubling down on buying more technical solutions.

Organizations appear to be failing across three main areas: 1) developing a long-term strategic risk-centric approach that fits with the globally changing political, sociological, and behavioral environments, 2) an over-reliance on technical tools and related training materials to more accurately and expeditiously identify an evolving threat, and 3) an overemphasis on employing technical rather than insider threat subject matter experts (SME). The results of this research seek to provide organizations with critical datapoints and examples that can be used to propose solutions so they can better address the actual root-cause of insider threats and not the symptoms and evolve their Insider Threat Programs (InTP).

1. Introduction

Prostitution is often referred to as the world's oldest profession (Duntley & Shackleford, 2008) while spycraft as the second oldest (Knightley, 1987). There is an entire chapter devoted to espionage in the *Art of War* which was written roughly 600 years before paper, 1,300 years before gunpowder, and 1,800 years before the compass were all invented. Deploying cloak-and-dagger clandestine tradecraft in order to gain insight into an adversary or competitor immediately conjures fantastic and romantic imagery of James Bond, Jason Bourne, and even Eli Cohen, who recently had a six-part series released on Netflix highlighting his exploits, victories, and ultimate capture and execution by Syria as he spied on behalf of Israel from 1961 to1965. While these stories are captivating, they are nowhere near accurate to the common use of intelligence gathering used by nation-states, competitive intelligence specialists, criminal organizations, and even the mass media.

The *Art of War*, written in the 6th Century B.C.E., states, "Knowledge of the enemy's dispositions can only be obtained from other men," (Tzu, 1963) and this is the challenge facing modern day security experts. Specifically identified by Sun Tzu as "Inward Spies," these are the insiders and the risk they pose to an organization. To the external party looking to gain insider knowledge, they do not care how the knowledge is gained and are more than willing to use any means necessary. Simply put, "Inward Spies" are people who share non-public information either maliciously or through negligence.

To counter these threats, current security strategies call for a seemingly never-ending stream of datapoints in an attempt to pinpoint the proverbial "bad" needle in the haystack. This has given rise to a global cybersecurity market currently estimated to be $173B, growing to $270B by 2026 (Forbes, 2020), and this does not include the annual $2.2B spent by the U.S. Department of Defense (DoD) for the Cyber Command (Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, 2020). Additionally, every U.S. college and university now offers both a bachelor's and master's degree in Cybersecurity yet most graduates lack the knowledge, skills, and abilities (KSAs) necessary to holisticaly apply security in cyberspace (Knutson, 2020).

Consequently, Chief Information Security Officers (CISOs) continuously call for more endpoint monitoring, network traffic analysis, baselining and normalizing of user activity, allowlisting, blocklisting, and still, from 2018-2020, the total number of insider-related incidents have increased by 47% (ObserveIT & ProofPoint, 2020). At what point in the annual budget spending and analyzing of insiders does industry realize and accept that the solution is not directly dealing with the problem at hand?

1.1. The Necessity, Reality, and Fallacy of Continuous Monitoring

The National Institute of Standards and Technology (NIST), Special Publication (SP) 800-37 described a Risk Management Framework (RMF) and provided guidelines for applying the RMF to information systems and organizations with an emphasis on risk management (NIST, 2018). A logical and comprehensive approach to risk is critical for every organization and constitutes the main value provided by any security-related department including Insider Threat Programs (InTPs).

Security departments are often referred to as “Cost Centers”, versus “Profit Centers”, and do not directly add to gross income but still cost the organization money to operate. As a result, is it critical for every security department to frame their organizational value in terms of risk to the company and, therefore, potential savings to bottom-line profit if a security incident is not mitigated. The risk is typically presented in many different ways including the risk of not collecting enough data points or not having the right analysis software and missing the key indicator of an impending attack. Along with other security frameworks such as the National Insider Threat Task Force Maturity Framework (NITTF, 2018) and the Intelligence and National Security Alliance Framework for Cyber Indications & Warning (INSA, 2018), NIST provides a solid foundation for the justification and onboarding of more monitoring tools and services as well as more headcount for cyber threat intelligence analysts to comb through the desert of data looking for a single grain of “bad” sand.

This approach was designed by and closely aligns with the typical personality type of those in the security field. Employees in this field tend to want more oversight, control, accountability, and well-defined lines of responsibility (Scullard & Baum, 2015).

This methodology worked well when insiders were identified post-attack. An attack generally brings anxiety, stress, panic, and fear and organizations need a calm, take-charge, communicative, dominant type of personality which is common in the security, law enforcement, and military fields. For this approach, the strategists matched the issue perfectly.

However, the desired framework has shifted to a risk-based model, giving birth to the Insider Threat or Insider Risk team as they try to move to the "left of bang" (Van Horne & Riley, 2014). The concept is solid: prevent an attack before it occurs therefore saving time, money, and lives. However, the concept has been doomed to failure as this new approach was designed and is now led by the same personalities and concepts of yesteryear. The security fallacy of today's Insider Risk team is that the "bang" still has to occur in order to be successful. The "bang" has to be almost imminent and, essentially, unavoidable. The insider has decided to commit the malicious act, either wittingly or unwittingly, which feeds the argument for deeper and continuous monitoring. Hence, security organizations are similar to Jack Bauer in the TV series *24* where the protagonists are charged with stopping guaranteed attacks at the last second. Depending on the point of view, the strategists either stayed laser-focused on the issue at the hand, the "bang", or myopic towards the root-cause — "bad people do bad things."

An age-old philosophical question is whether or not people are good or bad. A witting insider attack requires a conscious decision to wreak devasting consequences, sometimes even deadly, so it makes sense that witting attackers would be far less common. The 2020 Verizon *Data Breach Investigations Report* (Verizon, 2020) (DBIR) supports this assessment and explicitly states, "external attackers are considerably more common than internal." However, this is when the witting and unwitting insiders are considered separate groups and, by volume, the number of external potential attackers far outnumber insiders in any company or government. At present, there are approximately 7.7B people in the world who could represent the entire external attacker pool.

Ultimately, any external actor looking to gain internal access only needs one insider to grant them entry. Statistics on these types of attacks show that of one hundred phishing emails sent at a company, thirty are opened within four minutes. Of those thirty

over the next three minutes, four clicked the malicious link embedded in the text giving the attacker their first step of access to the machine (Verizon, 2018). For the lone criminal looking to exfiltrate credit card numbers or personally identifiable information (PII) for sale on the dark web, this is the easiest option available and was the likely attack vector for some of the largest data breaches in history: Adobe in 2013 (153M user records), Adult Friend Finder in 2016 (412.2M accounts), Equifax in 2017 (147.9M), LinkedIn in 2012 and 2016 (165M accounts), Marriott International in 2014 (500M accounts), and Yahoo in 2013 (3B accounts) (Swinhoe, 2021). Most external attackers and cyber criminals will fit into this category are not trusted employees and are unlikely to ever personally meet an employee who has trusted access. It is too easy and convenient to run these types of criminal operations at scale from the safety of a foreign country or basement.

However, for an industry competitor or nation-state looking to penetrate a stand-alone system behind a locked door, targeting, eliciting, recruiting, and exploiting a human asset is the only option and this is the discipline that was documented by Sun Tzu in the 6th Century B.C.E. Where the spearphishing attacks that lead to data breaches result in governmental regulations and fines, this type ends companies, alters industries, and even realigns the global balance of power.

1.2. The Necessity, Reality, and Fallacy of Security Budgets

In business, it is often said that there are two type of Centers: Profit and Cost. Profit Centers directly add money to the bottom-line profit of the business while Cost Centers do not add money and, instead, require money just to operate. Any support department is considered a Cost Center; Examples include Human Resources (HR), Legal, Engineering, Research & Development (R&D), Marketing, and Security. In order to grow budgets and headcount, security departments are always searching for facts and figures to help sell the unrealized savings of preventing an attack and the cybersecurity industry is happy to oblige with their own staggering numbers: $11.45M/incident (ObserveIT & ProofPoint, 2020), $8.19M/incident (Brook, 2020), $8.19M/incident (Tunggal, 2021), $551K/incident (Sjouwerman, n.d.), $3.92M/incident (IBM, 2020), $4B/year in U.S. (FBI Internet Crime Complaint Center, 2020). Whether it is the *DBIR*

(Verizon, 2020), *Global Threat Report* (CrowdStrike, 2021), or *M-Trends Special Report* (FireEye Mandiant, 2021), the marketing departments of these vendors are among some of the best in the world and there is always a Fancy Beary, BeZeeke, HondoFrog, or DancyDuck lurking right around the corner ready to wreak havoc.

Aligning perfectly with their security personality, CISOs rely upon reports and figures like these to influence their C-Suites and procure more headcount and budget for technical tools and solutions (e.g., Data Loss Prevention (DLP), Intrusion Detection Systems (IDS), Next-Generation Firewall (NGFW), User Behavior Analytics (UBA), etc.). The issue is that these reports and figures are published by marketing departments who rely on fear-based advertising: "Attackers don't break in, they login" (Beyond Identity, 2021), "Imagine a world without breaches" (Centrify, 2021), "The industry's only SaaS solution for enterprise DLP" (Digital Guardian, 2021), "Get left of breach/loss/compromise" (Forcepoint, 2021), "You need to secure every device on your network" (ForeScout, 2021).

In 350 B.C.E., Aristotle wrote *Rhetoric* and defined the modes of persuasion, or rhetorical appeals. Successful marketing campaigns satisfy all three of these appeals: ethos (ethics/trust/credibility), pathos (emotion), logos (logic) (Aristotle, 350 B.C.E.). Fear-based marketing is extremely persuasive because it leverages pathos to its highest degree and has even given rise to *FOMO* (Fear of Missing Out), a term coined in 2003 by Patrick McGinnis (Knowles, 2016), and *YOLO* (You Only Live Once) which was entered into the Oxford Dictionary as a word in 2016. Yet, despite the meteoric rise of cybersecurity vendors who are all fighting the same problem set, the problem persists and is growing. This is the necessity, reality, and fallacy of using fear to sell security as a Cost Center and it appears the only people getting rich from it are the cybersecurity vendors. Examples of these vendors are appended in Appendix A.

1.3. Societal Shift to Privacy and Its Impact on Cybersecurity

Professional Frameworks all advise for the installment and refinement of continuous monitoring solutions. At least six of the nineteen NITTF Maturity Elements (ME) all reference this type of solution (NITTF, 2018):

- **ME11**: Establishes a user activity monitoring (UAM) capability on all USG end points/devices and government-owned IT resources connected to USG computer networks accessible by cleared D/A personnel.
- **ME12**: Ensures UAM requirements are incorporated into D/A (departments & agencies) IT planning, design, and accreditation processes.
- **ME13**: Establishes capability to monitor the activity and conduct independent audits of InTP (Insider Threat Program) personnel with access to insider threat information and tools.
- **ME14**: Employs data integration methodologies and advanced analytics to help detect anomalous activity and potential insider threats.
- **ME15**: Employs behavioral science methodologies to help identify indicators of potential insider threat.
- **ME16**: Employs risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential insider threats and in the application of tailored mitigation strategies.

To follow the NITTF framework to a more mature model, InTPs seek to incorporate more datapoints which can then be analyzed with greater scrutiny. This has given rise to the latest cybersecurity trend, *Zero Trust* (Palo Alto Networks, n.d.). An evolution on the concept of *Need to Know*, Zero Trust is rooted in the principle of "never trust, always verify" and is the most security-intensive, restrictive, and privacy-shattering approach to date. Less trust and more monitoring have created workplaces with zero expectation of privacy and while this type of environment may be culturally acceptable in the most rigid and strict organizations (i.e., government, financial sector, energy industry) it is actually a self-fulling prophecy in terms of insider threats.

2. Evolution of Insiders, Threats, & Risks

2.1. People Problems that Manifest

Trusted insiders who ultimately betray their company or country likely share one common factor: unbearable stress. These insiders ultimately lash out and, due to the unique personalities of every individual human, it is impossible to predict how it will

manifest. However, generally speaking, there are six ways insiders have manifested. Some are more common than others, but all are a result of needing to relieve the unbearable stress and are effectively the only option the insider feels they have left:

- **Compromise** – Illegitimately gaining access to an otherwise off-limits area
- **Infiltration** – Legitimately gaining access to an otherwise off-limits area
- **Leakage** – Data or information exposure (numerous known details)
- **Espionage** – Data or information loss (numerous unknown details)
- **Sabotage** – Data or infrastructure damage or abuse
- **Violence** – Physical violence, active shooter, or self-harm

Predicting if, how, when, and where an insider will manifest is near impossible though those previously identified cybersecurity vendors will near guarantee their ability to accurately predict the "bang". Every person has a unique personality, and their predispositions are guided by the moral compass they innately have; though some research indicates one out of twenty are inherently lacking in the ability to manage their destructive behaviors (Stout, 2006). The issue is when people confront stressors that either singly or in totality become unbearable, they resort to behaviors in an attempt to alleviate the stress. Cybersecurity professionals are oftentimes logical programmers relying upon binary if-then-else statements to identify forward-predicting sequences and causation. Some likely believe that by collating singular datapoints into a technical monitoring and analysis system then they can predict, detect, and prevent insiders from manifesting. The flaw in this assessment is that the technical datapoints, or those that can be observed on the network, are only a small glimpse of the employee's activities and does nothing to deal with the issue before it has become risky or damaging. Appendix B, as modified from a U.S. Defense Counterintelligence and Security Agency (CDSE), DoD Insider Threat Management Analysis (DITMAC), is a common depiction used to describe the escalation process up a pyramid.

At the base of the pyramid are *Predispositions* which are the unavoidable characteristics that make people unique and human and are typically balanceable by stable, reasonable, logical, and calm adults. However, up one level are the *Stressors,* and

these are inevitable throughout their entire lives and collectively drain them mentally and physically. When *Stressors* reach an unbearable or unsolvable degree, people look to alleviate the stress through the *Concerning Behaviors*. At this stage, the well-balanced person can manage and may only exhibit a specific or certain behaviors. The issue is whether or not those *Concerning Behaviors* reach a point where they are inherently self-destructive or damaging to the company. A rudimentary example is that while a drink of alcohol may distract from a problem, repeated excessive drinking will lead to alcoholism. Note that 'Technical/Cyber' *Concerning Behaviors* is only a single type of data to help identify and detect an insider threat. The primary purpose of this pyramid is twofold: 1) to show the myopic approach to insider threat identification taken by cybersecurity, and 2) to show how dangerously close to manifesting an insider is when cybersecurity finally identifies technical *Concerning Behaviors*.

2.2. Technical Solutions for People Problems

In many cybersecurity departments, the definition of an insider threat is typically an authorized employee who somehow grants access to an unauthorized external entity, either wittingly or unwittingly. The *DBIR* considered this category to be 77% of all breaches (Verizon, 2020) and the top two attack vectors used by external entities were phishing and use of stolen credentials. The world's foremost hackers, the U.S. National Security Agency, whose stated mission is to "collect and report intelligence for foreign intelligence and counterintelligence purposes" (NSA, 2013), published a *Top Ten Cybersecurity Mitigation Strategy* document which, in essence, details the most efficient ways to stop them. The list is comprised of entirely basic security measures (NSA, 2018):

- Update and upgrade software immediately (so old and recycled passwords do not work)
- Actively manage systems and configurations (take inventory of what is allowed on the network, so database administrators inversely know what is not allowed)
- Segregate networks using application-aware defenses (if it's critical then compartmentalize it away from the normal traffic)

These cybersecurity countermeasures are technical solutions for people problems and are equivalent to more, and more secure locks. They address problems such as ignorance and negligence (i.e., unwitting insider attacks) but fall short of addressing either insiders bent on malice or the root cause that led to the insider deciding upon malice or falling for the trickery in the first place. They overlook a base tenet of espionage: "Don't steal what is given for free". Therefore, like most stereotypes, the assumption that an insider is accessing information they are not allowed to access is pure fiction.

At present, the only solution CISOs appear to have to confront phishing and poor password hygiene is standard check-the-box awareness training. Cybersecurity vendors are already prepared as this market is predicted to explode to $10B/year by 2027 (Morgan, 2020). Unfortunately, for a generation that was raised post floppy disks, modem dial-up connectivity, and COBOL (Common Business Oriented Language), warning them of these dangers is desensitized, forgettable, and as effective as saying "don't accept any wooden nickels" or showing them a Mr. Yuk sticker (University of Pittsburgh Medical Center, 1971). Providing awareness and education is key in raising any company's security posture but these risk areas are not the root of the problem, just symptoms. This type of training is likely to be received with the same level of apathy as all other annual training (Popov, 2015). Ultimately, to confront this growing issue, the industry is not asking the right questions, which are:

- What is the root-cause people problem that companies should address with the training?
- What makes a trusted insider truly susceptible to the trickery of phishing campaigns?
- What leads a trusted insider down their self-destructive path in the first place?

2.3. Case Studies & Research

Demonstrated in the pyramid in Appendix B, the cybersecurity industry generally defines 'insider threat' as the binary detection and mitigation of technical/cyber

concerning behaviors (i.e., when an employee uses a poor password or is duped into clicking on a phishing email), there is no data available on what was happening in the employee's life that led to them being targeted and therefore susceptible to the trickery in the first place. The SANS course *SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling* teaches the P.I.C.E.R.L. approach to incident response: Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned (SANS, 2016). Unfortunately, the lessons learned always ends with 'the end user clicked on a spearphishing email' which is a symptom of a deeper issue and not the root-cause.

This leads to more budget spending on technical solutions to gather more datapoints and conduct better analysis. This is the proverbial *pound of cure* rather than the *ounce of prevention*. The following case studies of verified insider threats are researched to ascertain if cybersecurity teams identified, detected, deterred, or mitigated the attacks or if the insiders somehow circumvented security countermeasures. The lesson has yet to be truly learned.

Open-source research and official findings and documents pertaining to these case studies are listed in Appendix C and many of these cases were investigated by the U.S. Department of Justice (DoJ) or the U.S. Department of Defense (DoD) pursuant to Title 18, U.S.C., Section 1832 (Theft of Trade Secrets), Title 18, U.S.C., Section 793 (Gathering, Transmitting, or Losing Defense Information), Title 18, U.S.C., Section 794 (Gathering or Delivering Defense Information to Aid Foreign Government) (United States Code, n.d.) or 22 USC, Section 611 (Acting as an Agent of a Foreign Power/Foreign Agent Registration Act (FARA)).

2.3.1. Paige Thompson, Capital One, Leakage

On April 21, 2019, Paige Thompson uploaded data from over 100,000,000 accounts and over thirty companies she had taken from Amazon Web Services (AWS) to Github, a free repository where over 40M software developers share code and other data. In this data, she included her full name and resume. In August2019, the DoJ charged her with wire and computer fraud. As an AWS software engineer, she was able to exploit a flaw in an application firewall stored on a cloud server to gain access to customer data belonging to a number of clients. Prior to the attack, she fretted on Twitter about her

dating life, mourned the euthanasia of her cat, struggled with her gender identify as a transwoman, and spoke darkly about her mental health, writing on July 5, 2019, that she intended to check herself into a facility for treatment. After uploading the compromised data to Github, a random user contacted Capital One to report a possible leak. Capital One confirmed the compromise and reported the issue to the Federal Bureau of Investigation (FBI) which led to the indictment. A key finding by the FBI was that Thompson was living in a house owned by Park Quan. Quan has a felony conviction from 1983 when he planted a bomb under a pickup truck – it did not detonate – and another from 1991 for owning a machine gun as a felon. In the residence, the FBI found a cache of weapons belonging Quan including an AR-15-style assault rifle, an AK-47-style assault rifle, scopes, gunpowder, and bump stocks all of which were readily accessible by Thompson.

This case study is included to demonstrate two key findings: 1) Thompson was not identified by any technical countermeasures, and 2) she chose to manifest with leakage (data or information exposure with numerous known details) versus violence, which was readily accessible from her roommate's firearms.

2.3.2. Major Nidal Malik Hasan, U.S. Army, Violence

On November 4, 2009, Major Nidal Malik Hasan, a U.S. Army psychiatrist, fatally shot thirteen people and injured thirty-two others aboard Fort Hood, TX. Major Hasan was arraigned by a military court on July 20, 2011 and was charged with thirteen counts of premeditated murder and thirty-two counts of attempted murder under the Uniformed Code of Military Justice (UCMJ).

From 2003 to 2009, when Major Hasan was stationed at Walter Reed Medical Center for his internship and residency, officials repeatedly expressed concern about his behavior and supervisors gave him poor evaluations, warning that he was doing substandard work (Chappell, 2013). As early 2008 and on later occasions, several key officials, including the Walter Reed Chief of Psychiatry, Chairman of the Uniformed Services University of the Health Sciences (USUHS) Psychiatry Department, and the Director of the psychiatric residency program reviewed Major Hasan's personnel file

which described him as “disconnected”, “aloof”, “paranoid", “belligerent” and “schizoid”.

Independent academic reviews and even a Congressional Special Report identified his Muslim radicalization and ideological beliefs as personal justification for the attack and offered his communications with Anwar al-Awlaki as evidence (Lieberman & Collins, 2011). Major Hasan was born Muslim but not raised religiously devout. However, following his mother’s death in 2001 after a long battle with cancer, he began to search for religion to help appease his suffering and found numerous contradictions between his family’s life and Muslim faith. He specifically blamed his parent’s decision to own a convenience store that sold alcohol, something forbidden by Islam, as evidence that his mother would never find solace in the afterlife. At this critical time in his life entered al-Awlaki, a Yemeni-American cleric and al-Qaeda propagandist, and Major Hasan listened fervently to his sermons on tape and came to gain “more insight into what it means to be at war with Islam, and how the US/West wanted a castrated form of Islam" (Poppe, 2018). These reports are influenced by the politics behind the radicalization that preyed on Major Hasan and subsequent *Concerning Behaviors* that should have been identified as warning signs – refer to Figure B - with only references as to *Stressors* where true help and avoidance could have been injected.

This case study is included to demonstrate that the over-reliance on technical monitoring had no effect on proactively identifying Major Hasan as an insider threat. There were multiple documented concerning behaviors in his records, and it is likely, but not verified, that his network activity included aspects that are indicative of his slow radicalization and propensity towards violence (e.g., Internet search results, email queries).

2.3.3. Ahmad Abouammo and Ali Hamad A Alzabarah, Twitter, Infiltration

On November 19, 2019, the DoJ charged three men with acting as agents of a foreign government and falsification of records: Ahmad Abouammo and Ali Hamad A Alzabarah who both worked at Twitter and Ahmed Almutairi, a representative of the Kingdom of Saudi Arabia. In 2013, an unidentified public relations firm representing the Saudi Embassy reached out to Abouammo, an employee with only six months' tenure, to verify an account belonging to a Saudi news personality. The conversation continued ultimately leading to an onsite personal tour for Saudi entrepreneurs at Twitter HQ and a meeting with another Saudi Representative, Bader Al-Asaker. In 2017, Abouammo met Al-Asaker in London, UK where he received a Hublot Unico Big Bang King Gold ceramic watch worth approximately $50,000.00. A week later, Abouammo accessed internal Twitter systems used to verify users and downloaded information related to two Saudi dissidents, including an email address, telephone numbers, and date of last login, which he provided to Al-Asaker. The two dissidents included a prominent critic with over 1,000,000 followers and an impersonator of the Saudi royal family. Over the next two years, Al-Asaker paid Abouammo over $300,000 and another Saudi representative, Almutairi, was introduced and replaced Al-Asaker. As the requests for more data grew, Abouammo realized he did not have the necessary access, so he introduced Almutairi to a colleague, Alzabarah, a Site Reliability Engineer (SRE) who had much greater access to more data. Their actions continued unbeknownst to Twitter until the FBI advised as to Abouammo's and Alzabarah's actions; how the FBI identified this activity is not publicly available. When confronted, Abouammo agreed to cooperate with the authorities. However, on December 2, 2015, Twitter management confronted Alzabarah, seized his laptop, put him on administrative leave, and escorted him from the building. Abouammo immediately contacted Al-Asaker who made the arrangements and the next morning Abouammo was on a plane to Saudi Arabia with his wife and daughter.

This case study is included to demonstrate that technical monitoring and analysis is ineffective in identifying the intent behind data access when the insider already has legitimate access to the data in the course of their regular duties.

2.3.4. Zhang Xiaolang and Chen Jizhong, Apple, Espionage

On July 16, 2018, the DoJ charged Zhang Xiaolang, an Apple engineer assigned to the secretive PROJECT TITAN team charged with researching autonomous driving vehicles, with stealing trade secrets. From April 1-8, 2018, Zhang traveled to the People's Republic of China (PRC) with his family while on paternity leave. Immediately after returning to work on April 30, 2018, he advised his supervisor he was resigning and intended to return to the PRC in order to be closer to his mother who was in poor health. During the conversation, Zhang advised he intended to find future employment with Xiaopeng Motors (XPeng), an electric vehicle company in Guangzhou, PRC with offices in Mountain View, CA and a direct competitor in the self-driving vehicle industry. Feeling as though Zhang had been evasive, his supervisor requested a forensic investigation by internal security which discovered Zhang's network activity had increased exponentially compared to the prior two years of his employment. They identified bulk searches and copious downloads of documents with confidential and proprietary information over the previous months. CCTV reviews identified Zhang accessing laboratories after normal working hours (9:00pm) and leaving with computer equipment that was not assigned to him. On June 27, 2018, Zhang purchased a one-way ticket to the PRC from San Jose for July 7, 2018 and he was arrested by the FBI as he passed through a security checkpoint.

Six months later, on January 11, 2019, Chen Jizhong, an Apple Hardware Developer Engineer, also assigned to PROJECT TITAN, was seen by a colleague taking photographs with a wide-angle lens inside a secure workspace that houses the autonomous driving project. An internal investigation found that Chen had recently advised his supervisor that he was traveling home to the PRC to care for his ill father and had recently applied for a role at an unidentified PRC-based autonomous vehicle company. The FBI searched Chen's residence where they found over 2,000 manuals, schematics, and proprietary files on his personal hard drive. The majority of the files were downloaded after his supervisor put Chen on a Performance Improvement Plan (PIP) earlier in the year. Chen was arrested on January 22, 2019, the day before he was scheduled to fly to the PRC.

This case study is included to highlight the importance of education and training which led to proactive reporting by employees. Both cases were brought to Apple's attention by studious and contentious employee: in Zhang's case, by his manager, and in Chen's case, by a coworker who identified suspicious behavior. Neither Zhang nor Chen was identified by technical countermeasures on the network.

2.3.5. Liu Ruopeng, Duke University, Espionage

From 2006-2009, Liu Ruopeng was enrolled at Duke University and worked on state-of-the-art metamaterials for Dr. David Smith, a professor of electrical and computer engineering. Specifically, Liu was working on the development of metamaterial cloaking and an invisibility cloak. Liu's work ethic and attitude endeared him to Dr. Smith and he grew into a protégé, though Dr. Smith would later refer to Liu as "bumbling a bit" (McFadden, Nadi, & McGee, 2018). During these years, Liu made frequent trips home to the PRC and, in 2007, convinced Dr. Smith to let him bring his "Chinese colleagues" into the lab as a special tour for personal friends. Unbeknownst to Dr. Smith and the university, through photos and measurements, the guests took the exact laboratory specifications and research. In 2010, Liu returned to the PRC and along with five friends founded Kuang-Chi Group, a Chinese company that develops and invests in metamaterial, telecommunication, aerospace, smart-city, artificial intelligence, and digital health technologies. In 2012, when Xi Jinping was elected President for Life in the PRC, the very first company he visited was the Kuang-Chi Group. In 2018, the Kuang-Chi Group was valued at over $6,000,000,000 and Liu has been called the "Elon Musk of China." To date, Liu has not been formally charged by the DoJ.

This case study is included to highlight how a general lack of knowledge or overall ignorance to this type of theft can lead to catastrophic impact on a global scale. The nature of this type of insider threat, espionage, is to appear to be benign, innocuous, and almost hinting that the stolen information is of little to no value making it a victimless crime. To many, the vision of criminality is very visceral and exoteric meaning it is easy for the layman to imagine the damage and everyone can generally agree that these actions are bad.

However, picture a developing nation openly declaring a national commitment to grow their economy by investing in technology and manufacturing. They then sponsor their best and brightest to travel the world and learn from innovators and entrepreneurs. After a period of education, apprenticeship, and growth, they return and apply their newfound knowledge at home finding a way to create a similar product or process. Ultimately, they build a globally competitive business by producing a competitive product cheaper, easier, and faster eventually putting the original innovators and entrepreneurs out of business. Is this not the purest form of capitalism? Where is the crime? This is the exact stated goal of the PRC's *Made in China 2025* strategic plan and this case study is an example of the economic impact (State Council, PRC. 2021) (U.S. Chamber of Congress, 2017).

2.3.6. Unidentified Employee and Egor Kriuchkov, Tesla, Compromise

On August 25, 2020, the DoJ charged Egor Kriuchkov, a Russian national, for his role in recruiting a Tesla employee to purposely inject malicious software, likely ransomware, into the company's computer network in an attempt to then extract sensitive data and extort the company. Instead of accepting the offer of over $1,000,000 for his support, the employee, who met Kriuchkov through an unidentified mutual acquaintance, reported the recruitment to internal security. Beginning on July 16, 2020, Kriuchkov entered the U.S on a tourist visa and contacted the employee via WhatsApp and made arrangements for an initial meeting in Reno, NV. Kriuchkov and the employee met from August 1-3, 2020 quickly becoming friends and Kriuchkov introduced the extortion attempt as a "business opportunity." Generally speaking, the plan was for the employee to introduce the malware to Tesla's network with either a USB thumb drive or email sent directly to him. This would then initiate an internal DDoS attack allowing the co-conspirators to upload ransomware from Russia. To date, Kriuchkov has not formally been linked to any nation-state organizations and the scheme appears to be entirely financially motivated by criminals.

This case study is included to highlight three key aspects in the targeting and recruitment of insiders: 1) recruitments are often framed in the context of "opportunities" to help the employee rather than the Hollywood version of blackmail or coercion, 2) the

concept of easy money is still a motivating factor, and 3) the attack was identified by the moral compass of the employee who was likely cognizant to this type of attack through effective training and awareness. There is no reporting or indication that the attack was identified by any type of cyber monitoring tool.

2.3.7. Andrew Levandowski, Waymo/Google, Espionage

In January 2016, Anthony Levandowski and three other employees resigned from Google in order to start up a self-driving vehicle company, Ottomotto, LLC. All four were assigned to PROJECT CHAUFFER, later renamed Waymo, Google's self-driving car project. Six months later, in July 2016, Ottomotto was acquired by Uber in a deal reported to be worth $680,000,000 and Levandowski assumed leadership of Uber's entire driverless car operation.

In March 2017, a case was referred to federal prosecutors and it was alleged that Levandowski "downloaded 9.7 GB of Waymo's highly confidential files and trade secrets, including blueprints, design files and testing documentation" which were then used to enhance Ottomotto's and Uber's self-driving vehicle programs (Hawkins, 2017). The internal Google investigation identified that Levandowski had downloaded 9.7GB of data two weeks prior to his resignation. On August 4, 2020, Levandowski pleaded guilty and was sentenced to eighteen months and over $800,000 in restitution for theft of trade secrets.

This case study is included to highlight the importance and efficiencies in monitoring and analyzing the entire employee lifecycle from onboarding to offboarding. Prior to announcing his resignation, Levandowski was not identified with any job dissatisfaction or leanings towards starting up his own competing company. After announcing his resignation, no efforts to restrict or analyze his final activities were undertaken and the compromise was only identified after an investigation that occurred several months too late.

2.3.8. Unidentified USG Employees and Jun Wei Dickson Yeo, U.S. Department of State, Infiltration

On July 24, 2020, Jun Wei Dickson Yeo pleaded guilty to one count of acting within the U.S. as an illegal agent of a foreign power. In 2015, Yeo, a Singaporean

national, was attending the National University of Singapore pursuing a PhD in Public Policy when he was recruited by a PRC-based Think Tank to write political reports and opinion pieces. Yeo would later be tasked to provide deeper and more detailed information, even referring to the type of desired non-public information as *scuttlebutt*. His research was entirely focused on political, economic, and diplomatic relations, first in Southeast Asia, but later solely on the U.S. To fulfill these requests, Yeo established his own consulting company, Resolute Consulting, and used LinkedIn to reach out to targets who self-identified the types of backgrounds from which he needed to gain scuttlebutt: DoD, national security, military, counterterrorism, security clearance, intelligence, defense, intelligence analysis, foreign policy, public policy, etc. To help obfuscate his activities and make himself appear legitimate, Yeo borrowed the company name from a company based in Houston, TX: Resolute Consulting Group, LLC.

The LinkedIn connections algorithm fed Yeo a steady stream of targets all of whom were seeking private sector employment and who were eager to sell themselves, sometimes even exaggerating their deep knowledge and access to sensitive U.S. intelligence. Targets were hired to provide short essays on Asia-Pacific relations, economics, and analysis and they were paid between $1,000-$2,000 per report. As the relationships evolved, Yeo would slowly ask for non-public information while also assessing the target's motivations and personal situations, specifically searching for financial and personal matters that could be leveraged and exploited. Three unidentified U.S. government officials were eventually targeted, elicited, recruited, and exploited by Yeo: a U.S. Air Force civilian with a Top Secret security clearance, a U.S. Army Officer assigned to the Pentagon, and an official in the U.S. Department of State. All confided in Yeo of their personal, financial, mental, or professional issues and Yeo, in turn, provided their resumes, backgrounds, reports, and personal stories to the PRC Intelligence Service that originally recruited him.

This case study is included to contrast the obvious recruitment-in-place (RIP) used by Kruichkov to target Tesla and the seemingly benign and innocuous approach which is likely more common by attackers. Ryan Clarke, a senior fellow at the East Asian Institute, a Singapore-based Think Tank, stated, "These types of operations are quite simple with relatively few moving parts, which is why they are replicable at scale. The

general approach is to establish target priorities and then proceed to collect what appear to be rather innocuous inputs with relatively limited value when viewed in isolation. Sometimes the information may not even be classified" (Bowie, 2020).

This case study is similar in structure to the DoJ case against Kevin Mallory, formerly employed by the U.S. Central Intelligence Agency (CIA). Mallory was arrested in May 2019 after being recruited via LinkedIn by a PRC-based Think Tank and eventually agreeing to sell sensitive and classified information to the group to help relieve the stress of over $1,000,000 in debt (mortgage, credit cards, home equity line of credit). Mallory was initially identified by the PRC Intelligence Service (PRCIS) from his LinkedIn profile which overly hyped his background in the Intelligence Community (IC).

2.3.9. Jin Julian Xinjiang, Zoom Media Communications, Sabotage

On December 18, 2020, the DoJ filed a criminal complaint alleging Jin Julian Xinjiang collaborated with PRCIS to silence the political and religious speech of Zoom Video Communication (Zoom) users. Zoom is a U.S. company and Jin was the PRC-based Security Technical Leader and primary liaison to law enforcement and intelligence services. Officially, his role was to prevent users from using the platform for illegal activities. Jin fabricated Terms of Service (TOS) violations to provide justification for terminating meetings and even some personal user accounts. Jin set up an anonymous email account to report that the hosts in the meetings were supporting terrorist organizations, inciting violence, or distributing child pornography and then formally sent it for review, which was delivered to him through normal processes. Upon receipt, Jin was able to task engineers to terminate the meetings and accounts when, in fact, the meetings were intended to discuss democracy and the June 4, 1989 Tiananmen Square massacre. Ultimately, though he could not dial into the meetings or record the conversations, Jin's role allowed him to identify meetings deemed by the Chinese Communist Party (CCP) to be "illegal" which included meetings about political and religious subjects.

This case study is included to demonstrate the importance of customer data segregation and obfuscation from trusted insiders. Similar to the targeting of Abouammo at Twitter, insiders who are granted access to sensitive data, specifically customer

content, are at risk of the targeting, recruitment, and exploitation by sophisticated actors such as nation-state-trained intelligence officers. Following the Abouammo incident, a Twitter employee commented, “The people running onboarding didn’t do much training in terms of the specificities of the challenges that we would be facing. Nobody told us that we would be approached, that we would be — I don’t know if ‘seduced’ is the right word — that we would be intimidated into giving any kind of Twitter information” (Kantrowitz, 2020). Therefore, it is critical that training and awareness are presented in a culturally acceptable way that presents the employees as victims and not perpetrators.

2.3.10. Walter Lian-Heen Liew and Robert Maegerle, Dupont/Chemours, Espionage

On March 5, 2014, a federal jury convicted two individuals and one company for the first time under the Economic Espionage Act of 1996. Walter Lian-Heen Liew (aka Liu Yuanxuan); his company, USA Performance Technology Inc., and Robert Maegerle conspired to steal trade secrets from E.I. du Pont de Nemours & Company. Specifically, the two men stole the technology and research and development (R&D) behind titanium dioxide (TiO2) which, after refinement, produces the perfect color white and is used in thousands of products globally from refrigerators and cars to cosmetics, Oreo cookies, and even the pages of the Bible. DuPont/Chemours had gone to great lengths to shield the TiO2 process from theft: security guards, tall fences, escorts for visitors, forbidding photography, bag inspections, documents and blueprints that must be signed out and are maintained on segregated internal-only networks, and confidentiality agreements. Liew, a naturalized U.S. citizen with a master’s degree in electrical engineering from the University of Oklahoma (1982), was described by friends as ambitious with a dream of running his own company. In 1991, he was invited to a banquet in the PRC where he was celebrated as a “patriotic overseas Chinese” and returned to the PRC numerous times over the next twenty years to attend more banquets in his honor and to recognize his greatness. In 1997, Liew recruited Maegerle, a retired Dupont Mechanical Engineer who provided the additional internal information on how to build a TiO2 refinement plant. The two contracted with the Pangang Group Company Ltd, PRC and won three contracts worth $28M.

This case study is included to highlight a common recruitment tactic that goes almost entirely undetected by modern cybersecurity tools and techniques: the flattery of ego. As Liew's aspirations and ego led him to seek more wealth, prestige, and recognition, the recruitment began with a simple banquet in his honor. The details for Liew are similar to the March 2018 DoJ indictment of Xu Yanjun. Over several years, Xu identified subject matter experts in the aviation and aerospace industries, recruited and paid them to travel to PRC universities as distinguished guests, and convinced them to inadvertently reveal trade secrets. Xu was a suspected PRC Ministry of State Security (MSS) officer. The MSS is responsible for counterintelligence, foreign intelligence and political security and has been described as one of the most secretive intelligence organizations in the world.

2.3.11. Turab Lookman, Los Alamos National Laboratory, Leakage/Espionage

On September 15, 2020, Turab Lookman was sentenced to five years' probation and a $75,000 fine for false statements regarding his involvement with the PRC Thousand Talents Program, a governmental program established in 2008 to recruit international experts in science, research, and business through exchanges and funding.

On July 7, 2020, FBI Director Christopher Wray advised that this program has been linked to dozens of economic espionage investigations including at Texas A&M University, Harvard University, the U.S. National Oceanic and Atmospheric Administration (NOAA), and Phillips 66 which had proprietary information valued at over $1B stolen by employee Tan Hongjin in November, 2019 (Taylor, 2020). In each of these cases, the employee was not initially a nefarious insider looking to steal information they did not already have access to in the first place. They were approached by an external entity for the purposes of educational and professional networking. Using one of the thirteen different elicitation techniques as taught by intelligence agencies, examples are included in Appendix D, the experts are slowly coerced to share more and more details regarding their research, background, insight, or expertise. Elicitation is merely conversation with a purpose/goal and intelligence agencies formally train in these tactics,

techniques, and protocols (TTP) effectively transitioning the employee into prey with a goal of exploitation.

Lookman was approached by representatives of the PRC Thousand Talents Program who eventually offered funding and he was indicted not on his relationship with the PRC representatives but rather by lying about the mere existence of the relationship. No known intellectual property was leaked or stolen but the case identifies the intent to recruit on behalf of a nation-state targeting information outside the realm of national security.

This case study is included to highlight a similar but much more sophisticated approach as that taken by Yeo via LinkedIn. Like Yeo, the representatives specifically targeted Lookman and relied upon his ignorance, ambivalence, and naivety to the threat to start the seduction, followed by assessing which motivation can be exploited to gain greater inside knowledge (e.g., money, ideology, compromise, ego). Though there was no known compromise, the targeting and recruitment was in no way identified by cybersecurity technical countermeasures.

2.3.12. Simon Lancaster, Apple, Compromise/Leakage/Espionage

In March 2021, Apple sued Simon Lancaster, a former Materials Lead, for accessing trade secrets outside of his job's scope and then selling it to a media correspondent.

Since 2018, Apple experienced numerous leaks citing an "internal source" but was unable to identify Lancaster until he resigned, and an internal investigation reviewed his company-issued device. At that time, Apple investigators not only confirmed the access to leaked documents but also the correspondence with the journalist who reported the information. Additionally, only then did investigators realize Lancaster had downloaded a "substantial number" of confidential documents onto his personal computer which would be of value at his new employer, Arris Composites, a materials company in Berkeley, CA. This downloading was specifically requested by the journalist one day after Lancaster submitted his notice of resignation, October 15, 2020. The amount of money Lancaster received from the journalist is unknown and if the Arris Composites job offer was contingent upon bringing the trade secrets from Apple. In a

November 2019 post on LinkedIn, Lancaster posted “Why I left Apple and joined Arris Composites” and stated, "I was able to step up and help the engineering product design department take sketches off the drawing board and turn them into real products…I fell in love with the magic of certain processes, like additive manufacturing and composites, and would stay on to become Apple's advanced materials lead" (Brodkin, 2021).

Apple is renowned in industry for its ability to protect secrets and strategically release information in a way that generates customer excitement and loyalty. This case study is included to demonstrate that despite industry-leading security measures, even Apple is susceptible to an insider attack and what might have been available internally, but is not publicly available, is the analytic intersection between cybersecurity (i.e., Lancaster’s network activity), HR (i.e., Lancaster’s performance), and Physical Security (i.e., Lancaster’s physical activity on campus).

2.3.13. Dejan Karabasevic, American Superconductor, Inc., Espionage (July, 2018)

On July 6, 2018, PRC-based wind turbine company, Sinovel Wind Group LLC, was given the maximum fine possible, $1.5M, for stealing trade secrets from American Superconductor, Inc. (AMSC). Sinovel’s Deputy Director of R&D, Su Liying, and a Technology Manager, Zhao Haichun, convinced Karabasevic, Head of AMSC Windtec’s automation engineering department to resign and assume a similar role with Sinovel based upon sensitive source code he downloaded and stole. Since first meeting with Su and Zhao, Karabasevic accepted numerous paid business trips to the PRC, a five-year contract at twice his current pay (~$2M), at least $20k, a promise of “all the human contact” he wanted including “female co-workers”, and a whole new life in the PRC. In the year prior to this, Karabasevic separated from this wife and was demoted to the Customer Service Department and told colleagues that he felt “undervalued.”

In a March 23, 2018 interview, AMSC CEO, Daniel McGahn, stated AMSC started a business relationship with Sinovel in 2007; Sinovel manufactured the wind turbines while AMSC designed the technology that powered them. In this venture, Sinovel was AMSC’s largest client accounting for 67%-70% of total revenue from 2008-2010. In 2011, Sinovel owed AMSC $70,000,000 for a shipment that it had already

received. When they refused to pay, AMSC's stock price was halved and they lost nearly $1B in shareholder equity overnight. Over 700 employees were eventually laid off. In 2010, AMSC's total revenue was $315,955,000 and by 2015 it had plunged to $70,530,000 all in response to Sinovel acquiring AMSC's intellectual proprietary source code via Karabasevic, replicating the process, and replacing them within industry. In 2016, Sinovel reported that they had passed General Electric as the world's second largest wind turbine maker with a total revenue of $944,660,000. As of 2020, AMSC's total annual revenue is $63,840,000 compared to Sinovel's $628,660,000. In 2018, CEO McGahn felt that the "[Sinovel] strategy was to kill us."

This case, and others, has been used to provide continuing long-term evidence of the PRC's commitment to espionage above and beyond the traditional target of national security. In an opinion article of The Wall Street Journal on December 3, 2020, the U.S. Director of National Intelligence, John Ratcliffe, formally addressed the PRC strategy of "rob, replicate and replace" as the "greatest threat to democracy and freedom world-wide since World War II" (Ratcliff, 2020). On July 7, 2020, FBI Director Christopher Wray stated the FBI was opening a new PRC-related counterintelligence cases about every ten hours (Wray, 2020). Ratcliff identified the PRC strategy of stealing intellectual property from other countries, replicating the technology, and ultimately replacing them in the global marketplace.

This case study is included to highlight the impact and damage a single insider can cause and that the root of the matter stems from the personal and professional stressors each and every employee encounters. Karabasevic was not initially financially motivated but used money, title, and prestige to rationalize and justify his actions. The impetus for his actions stemmed from his unhappiness and disgruntlement towards his role, access, and impact which were then compounded by personal family crises. Employees are not capable of separating work and personal lives and feel the pressures and stress from each simultaneously and ultimately lash out in one environment or both.

2.3.14. Ryan Hernandez, Nintendo Co. LTD, Leakage

On December 1, 2020, Ryan Hernandez was sentenced to three years in prison for federal crimes related to his hacking of Nintendo Co., LTD and possession of child

pornography. Four years prior, while still a minor, Hernandez phished Nintendo when he posted a malicious link on the company's official and public forum requesting help with a technical issue. The link redirected the technical service representative to an external website where they were infected with malware. Hernandez was then able to scrape the employee's information and authentication credentials and used those to upload additional malware to the internal development network which logged the tokens of thousands of users. He later gained administrator access and began downloading proprietary data including pre-release information which he then leaked to Twitter and Discord using the moniker "RyanRocks" and online form "Ryan's Underground Hangout." An internal investigation by Nintendo led to an FBI referral which led Hernandez' arrest.

This case study is more closely aligned to the perception and definition of cybersecurity attacks where an external entity, such as Hernandez, uses trickery to compromise an insider's machine. The insider was not specifically targeted via social engineering or a spearphishing email and falls into the unwitting category previously cited by the DBIR. The main aspect to highlight in this case study is the ease of cyberspace attacks thanks in part to the simplicity of open-source tools such as Metasploit and Kali Linux.

2.3.15. Eric Swalwell, U.S. Congress, Infiltration

On December 8, 2020, Axios Media, Inc., a news website, published a bombshell expose reporting Christine Fang (aka Fang Fang) had infiltrated the U.S. political landscape through fundraising and sexual affairs with several politicians. In 2011, Fang graduated from California State University East Bay where she served as President of the school's Chinese Student Association. University Chinese student organizations, typically members of the Chinses Students and Scholars Associations (CSSA), were identified in 2018 as prime targets for PRC influence and intelligence activities as they maintain close ties to Consulates (Allen-Ebrahimian, 2018). Between 2011-2015, Fang established a close relationship with numerous politicians including Congressman Ro Khanna, Fremont Mayor Lily Mei, Senator Bob Wieckowski, Dublin Mayor Melissa Hernandez, Assemblywoman Judy Chu, Cupertino Mayor Gilbert Wong, and

Assemblyman Mike Honda. Additionally, Axios reported Fang had sexual relationships with two unnamed Midwestern mayors.

One of Fang's most controversial relationships, however, was with Congressman Eric Swalwell. From 2013-2014, Fang was deeply involved with campaigning and fundraising for Swalwell's 2014 reelection bid. In 2015, Swalwell was appointed to the U.S. House Intelligence Committee and Chief Democrat on the CIA's Oversight Subcommittee. These political assignments grant Swalwell extensive insight and knowledge of classified intelligence and on December 9, 2020 Swalwell vehemently denied sharing any classified information with Fang (Cohen, 2020). Ultimately, Fang was identified — not through security awareness training or through the exploitation of Swalwell — but by an FBI referral where she was observed in close proximity to a previously known PRC intelligence officer.

This case study is included to highlight the value and importance of non-classified, non-proprietary information to competitors and nation-states. The FBI advised that the goals of Fang's infiltration were twofold: 1) learn the demeanors, attitudes, behaviors, and opinions of future senior politicians in order to have an earlier and clearer understanding of how they will respond and react, and 2) influence those attitudes, behaviors, and opinions in a way that is more sensitive to and aligned with PRC objectives. This type of longer-term intelligence operation is not uncommon and has been documented in Silicon Valley numerous times (Dorfman, 2018) including in February 2018 when the personal driver for U.S. Senator Dianne Feinstein was investigated for suspected ties to the PRC MSS. Additionally, the expansion of Chinese culture, for example via Confucius Institutes, has been identified by some as a soft and deliberate attempt to slowly desensitize the west as to the nature of nefarious governmental intelligence operations (Grassley, 2018) (Grassley, 2020).

3. Data Analysis

Historically, the goal of InTPs is to prevent, detect, and deter employees from either engaging in risky activities or outright causing damage to the company, both wittingly and unwittingly. Finding the motivation of the insider and comparing that with

a common method of technical discovery, within reason and context, can help evaluate the efficacy of those programs, as seen in Appendix E.

Each case study is slightly different, but they all share two common themes. First, each is traceable back to at least one of the four primary motivations why counterintelligence officers believe insiders make the final decision to betray their employer: 1) money, 2) ideology, 3) compromise, and 4) ego (Volkman, 2008). Second, while it is assumed each of these companies have robust cybersecurity departments none were preemptively identified through cyber means.

For all, there are a number of behavioral indicators that could have been captured and potentially identified these insiders including: suspicious travel (unreported, foreign, expense-free, non-business/personal or side business-related), suspicious communications or contacts (new friendships or relationships with strangers), declining work performance (assignment to a PIP), job hunting or career searches or career advancement, and reports of misconduct to HR.

All of these indicators are collectible through a combination of technical and non-technical means. Some of these might include: emails to external accounts, collaboration with internal HR departments, physical security (badge records), web traffic to job and career sites, travel, financial relief, addiction and rehab, and dating sites, introduction of external media or personal cloud accounts to network devices (USB, Dropbox, G-Drive), internal document scans for files resembling resumes or CVs, or manifestos of disgruntlement. But, as none of these cases were preemptively identified by InTPs, there was likely a breakdown in one of three areas: collection (i.e., datapoints not being collected), technical analysis (i.e., data analysis tool inefficiencies or failures), or analyst assessment (i.e., lack of expertise and experience of the analysts themselves).

3.1. Method of Discovery

Once the companies knew who to investigate and what to look for, generally speaking, their internal Incident Response and Computer Emergency Response Team (CERT) was able to collect and document the necessary evidence for federal authorities to bring formal charges. This was observed in the Paige Thompson (AWS), Zhang Xiaolang (Apple), Andrew Levandowski (Google), and Dejan Karabasevic (AMSC) case

studies. Of significant note, three cases were identified by the quick thinking of colleagues who recognized abnormal behavior and reported it to their internal security teams: Unidentified Employee (Tesla), Chen Jizhong (Apple), and Kevin Mallory (CIA).

Each company employs a senior-level executive responsible for overseeing and ensuring information assets are adequately protected, which is typically the CISO, and they oversee the Security Operations Command/Center (SOC). The role of the SOC is to continuously monitor the company's internal networks in order to prevent, detect, and analyze cybersecurity incidents. In the DoD, this function is managed by the U.S. Cyber Command (USCYBERCOM). In short, the primary role of the SOC is to prevent these insiders before they download, compromise, exfiltrate, or otherwise abuse their access. None of them, in these case studies, were proactively successful.

3.2. Datapoint Analysis Gaps

The critical gap in data analysis can likely be attributed to one or more of three areas: initial collection, analysis tools, expertise of analyst.

The collection of datapoints is an easily definable requirement that is much harder in practice. Different technical datasets are maintained in different structures, formats, and even coding languages. Organizations have been trying to find a common ruleset and format dating as far back as 1996, when the Extensible Markup Language (XML) was first introduced, and it is still a common problem when onboarding any new tool. Additionally, many security departments and InTPs run into administrative roadblocks over the privacy and usage of sensitive data as merely sharing it with security sometimes goes against an open, free, honest, and transparent culture.

The second area of likely breakdown is in the tooling with the collected data. There are a massive number of applications and tools that tout their ability to import, analyze, and identify the threats with accuracy yet no one has proven to be any more of a gold-standard beyond their competitors. Building or buying a User Behavior Analytics (UBA) or User and Entity Behavior Analytics (UEBA) tool has become a top priority for many CISOs and has come to represent a figurative Holy Grail for InTPs.

The third area of likely breakdown is in the analyst themselves and the biases they inherently bring. Throughout his almost seven decades with the U.S. Intelligence Community (IC), Richard Heuer developed the *Analysis of Competing Hypotheses* and in it he identified six common biases that impact every analyst: anchoring/focusing, confirmation, congruence, hindsight, illusory correlation, and *cum hoc ergo propter hoc* or correlative and casual confusion (Heuer, 2019). Heuer laid out a structured seven-step process to assist analysts, detailed in Appendix F.

A breakdown in this area is not likely due to the analysts being unintelligent or unable to pivot from one datapoint to another. Throughout industry, most education and experience in analysis is focused on clearly identifiable cyber threat indicators such as hash values, IP addresses, port numbers, email addresses, domain names, network/host artifacts, and tools. The breakdown is more likely due to the analyst's background and experience being tuned these cyber-specific datapoints and not to the TTPs of the intelligence discipline.

On this point, the four primary motivations – money, ideology, compromise, ego – often referred by the acronym M.I.C.E., have long been the standard for understanding why someone would betray their employer or country (Charney & Irvin, 2016). These are used both by counterintelligence teams to understand how to defend against penetration as well as foreign intelligence teams to understand how to persuade someone to work on their behalf (Department of the Army, 2013) (Department of Defense, 2017). Examples of counterintelligence agencies that defend against the perpetrators are the FBI, U.S. Air Force Office of Special Investigations (AFOSI), and U.S. Naval Criminal Investigative Service (NCIS). Examples of foreign intelligence agencies that look to recruit and exploit are the U.S. CIA, PRC MSS, and Russian Federal Security Service (FSS) – the successor to the Soviet Union's Committee for State Security (KGB). However, while these four (MICE) are often cited as the primary motivation for the insider's behavior, the relationship of predispositions, stressors, and concerning behaviors prior to the insider making the ultimate decision to lash out, is often what is neglected. This is previously referenced in Appendix B.

In 2013, David Bianco proposed *The Pyramid of Pain* which visually contrasted the simple cyber indicators (e.g., hash values, IP addresses, domain names) with the most difficult to obtain, the TTPs (Bianco, 2014). The Pyramid of Pain is graphically represented in Appendix G. To date, there are numerous training facilities that teach how to collect and analyze the less painful indicators such as KnowBe4, Digital Defense, Habitu8, Cofense, CybSafe, Cybrary, and Broadcom (Symantec). But there is only one publicly available training facility that provides an education on intelligence TTPs, The Centre for Counterintelligence and Security Studies (CI Centre). However, the CI Centre's courses rely almost exclusively on U.S./Soviet Union Cold War-era examples, case studies, and TTPs and falls short of a cyber nexus. Simply put, cyber threat analysts have been trained to interpret one language (cyber datapoints), yet the adversaries are speaking in something else that is entirely foreign (intelligence tradecraft).

For example, the network detection tools capture when a user introduces external media like a USB thumb drive to a laptop and an analyst might see this as an issue, briefly investigate deeper, and ultimately decide not to escalate because no sensitive data is downloaded. However, a background or education in intelligence would assist this analyst in asking follow-up question such as:

- Was this the first time this specific USB had been introduced?
- When was the last time a USB had been introduced and was that also the first time it had been introduced?
- Is the employee expected to take leave in the next coming weeks?
- To where does the employee's company-issued device (e.g., mobile phone) travel in the following days or weeks?
- Are there any indications that the employee is undergoing personal or professional stress or anxiety?

Data sought by competitors and intelligence services is not always top secret or proprietary and even the mundane, outdated, expired, and innocuous can all be extremely valuable. The Eric Swalwell case study is an example of where a foreign intelligence service sought exactly this type of data.

4. Current State and Future State Recommendations

Intellectual property (IP) is part of what makes a company unique, competitive, and successful. To protect their IP, every company employs a security team charged with investigating attempts to abuse or steal that IP. However, investigations are inherently reactive in nature as they require the undesirable activity to occur so they can begin to collect relevant facts and details. Whether it is placing security guards at doors to search bags or having analysts sitting in the SOC watching the network traffic leave the ecosystem, every scenario culminates at the final stages of the insider's decision to betray the company. This is akin to a Secret Service Special Agent diving in front of the U.S. President to take a bullet after the gun has already been fired and though this may work in the movies, it is unlikely to be successful long-term. The threat must be realized for the security team to respond so protecting IP in this manner can be thought of as the first stage of protection and simply referred to as 'Threat'. This makes the second stage of protection, where companies seek to identify pre-attack indicators, as 'Insider Threat'.

4.1. Current State

'Insider Threat' is the first step of moving to the "left of bang" with the goal of identifying threats earlier. However, this stage implies that the insider has still made the final decision to commit the act the threat is unavoidable. Though this 'Insider Threat' stage is sooner than the previous 'Threat' stage, it is still doomed to failure and industry wants to move further "left". Consequently, industry is investing in more AI/ML to get more detailed IAWs creating the latest stage, 'Insider Risk'.

Several years ago, Lockheed Martin, a U.S. aerospace and defense contractor valued in 2020 at $59.81B, developed the *Cyber Kill Chain* framework (Lockheed Martin, 2015). A seven-step process, it follows the likely stages of an adversary with the goal of helping analysts and investigators identify possible intrusions and attacks earlier in the Chain to help them move their posture more to the "left of bang" (Van Horne, & Riley 2014). The Cyber Kill Chain's seven steps are 1) reconnaissance, 2) weaponization, 3) delivery, 4) exploitation, 5) installation, 6) command & control (C2), and 7) actions on objectives. The Cyber Kill Chain is graphically depicted in Appendix H. To support this methodology, the industry has leaned heavily on artificial intelligence and machine

learning (AI/ML) to help identify pre-attack indicators and warnings (IAW) earlier in the framework giving rise, first, to the concept of 'Insider Threat' and, now, to 'Insider Risk'.

If 'Insider Threat' is *pre-threat* then 'Insider Risk' is the *pre-pre-threat* stage. The goal is to have AI/ML analyze millions or billions of datapoints on the network in order to predict the threat based upon the risky behavior by the employees. This type of analysis is based on a model in criminal justice called Criminal Spin (Ronel, 2011) and was formally presented in 2005 by Professor Natti Ronel, Department of Criminology, Bar-Ilan University, Israel. The concept is that a criminal begins their negative behavior with relatively small acts, oftentimes without malicious or criminal intent, but it starts an inevitable chain-reaction of decisions where their actions escalate in severity. A rudimentary example might be if the 'Threat' stage is when an employee resigns then the 'Insider Threat' stage is identifying when that employee Is spending six hours per day on job hunting websites. The 'Insider Risk' stage is then when they are spending three hours per day job hunting. At the 'Insider Risk' stage, the activity is indicative of an employee who is considering leaving the company, but they have in no way truly made the ultimate decision that their career with this company has ceased to be productive.

The next stage, which has not been fully realized within industry, will be 'Insider Pre-Risk' and it is likely going to be predicated on collecting even more and better detailed IAWs so as to move further "left". The analysis and decisions made by AI/ML at this point will likely be so far left that the false positive rate will be astronomical and unscalable. From the previous example, the same employee is now spending one hour per day on job hunting websites.

This deep analysis is very invasive, and it appears society writ large is moving in the opposite direction, to more privacy-focused applications and open and transparent management and reporting. The European Union's General Data Protection Regulation (GDPR) passed in 2016, the California Consumer Privacy Act (CCPA) passed in 2018, and the rise of End-to-End-Encryption (E2EE) by many online applications such as WhatsApp, Facebook, Zoom, Telegram, and Signal are all geared at protecting consumers, and in some jurisdictions, employees also, their personal data. This stage is likely to be short-lived setting the stage for the desired future state, 'Insider Protection'.

4.2. Future State Recommendations

As the frequency and impact of attacks with an insider-nexus is escalating seemingly daily, it is unlikely the structure and framework of past and current InTPs will show scalable and effective success. The reactive and punitive approach currently deployed is the proverbial *pound of cure* and InTPs would benefit by finding the *ounce of prevention*.

The root-cause of the threat does not appear to be in a lack of technical resources, network compartmentalization, access controls, password hygiene, or even awareness training. These are all being developed, purchased, and deployed on a global scale to the tune of a near literal *moonshot* of funding annually. Industry has long considered the workforce first as the threat and now as a risk. This sends a negative message that has proven to be self-fulfilling. Employees are treated as threats, so they feel as though they are an untrusted threat and, in turn, become one.

The root-cause appears to be in the two constant features among all insiders: unhappiness and a gradual descent over time. Every single insider has documentable instances of being overworked, underpaid, under-appreciated, and a feeling of being trapped and isolated with no good option on the horizon. The emotional state of these employees is not all that dissimilar from the six symptoms of Battered Woman Syndrome (BWS), which has been identified as a subcategory of posttraumatic stress disorder (PTSD): 1) intrusive recollections of the trauma event(s), 2) hyperarousal and high levels of anxiety, 3) avoidance behavior and emotional numbing (i.e., depression, disassociation, minimization, repression, denial), 4) disrupted interpersonal relationships, 5) body image distortion and/or somatic or physical complaints, and 6) sexual intimacy issues (Walker, 2009) (Walker, 2016) (Whiting, 2016).

The negative biological effects caused by hostile work environments, roles with no scope for growth or promotion or mental stimulation, and even micro-management are the strongest contributors to the slow mental descent of an insider. These types of environments lead to heightened levels of cortisol, which is to the human body as driving a car with the RPMs (revolutions per minute) in the red and can be highly detrimental to the engine over time (Sinek, 2014). Appendix I is appended as a graphic representation of

RPMs running dangerously in the red. Biologically speaking, cortisol is meant to be injected into the system at a moment of stress and then flushed when the danger has passed. However, workplace environments that allow cultures based on zero-trust, continuous monitoring, and micromanagement lead to high anxiety and stress, which leads to a constant and heightened level of cortisol, which leads to less empathy, compassion, generosity, and sympathy, which leads to the slow descent of an insider. Given this chain reaction, collecting more datapoints and building better data analytic tools is only marginally likely to identify the threat sooner and much more likely to foster and nurture an environment conducive to insider threat behavior.

Consequently, establishing an InTP that is structured, presented, communicated, and deployed as a wellness program will be better received and, ultimately, more impactful than any reactive, security-first investigative team. It is estimated that 33% of Americans show signs of clinical anxiety or depression (Clifton, J. & Harter, J., 2021) and InTPs should interpret this figure that 33% of their workforce are in an environment that is causing them to trend towards being a threat. Globally, since the emergence of the COVID-19 pandemic in early 2020, the wellness topic of *resiliency* has emerged as a drumbeat of strength and many companies are starting to employ a Chief Resiliency Officer. Wellness is the ounce of prevention for which InTPs have been searching.

For years, security departments have used catchy slogans to encourage proactive reporting: “It’s okay to say”, “See something, say something”, “If you suspect deceit, hit delete”, and “Think before you click”. All of these slogans are aimed at identifying incidents just prior to bang (i.e., Insider Threat or Insider Risk). To think ‘wellness’ rather than ‘security’ would change the feel of the slogans to something like “It’s okay to not be okay”, “We’re here to listen”, “We’re here to hear”, or “When you’re sad or mad, think of us as dad”.

Establishing an InTP based on positive, proactive outreach that educates employees and encourages positive behaviors rather than punishes negative is key to long-term success. The education should center around viewing the employees as targets and victims of external predators who will prey on them when they are at their most vulnerable. Educate the workforce to what it smells, sounds, and feels like to be targeted,

approached, elicited, recruited, and exploited. In this context, regular education is different than annual security training as it is more akin to taking a vitamin every day rather than working out once a year. It will have longer term positive effects and build trust and goodwill between the workforce and the InTP. This type of approach will allow insiders to have difficult days and experience stressors without the fear of stigma or punishment. Challenges and stress cannot be eliminated from life and this type of approach normalizes those and creates a trusting relationship with security so that employees know what to do when they are at their most vulnerable and the external sharks start to circle.

Some of the most critical partners and InTP needs to liaise with are Internal Comms and HR. Tailoring the program in an entertaining and whimsical manner that is culturally acceptable will make the message palpable to the workforce. Specifically, partnering with HR can identify which teams, employees, and departments are most at risk due to low morale and high anxiety as well as which have access to sensitive data and IP (INSA, 2020).

5. Conclusion

The risk posed by insiders was formally documented 600 years before the invention of paper. Having a team strategically positioned and primed to detect, deter, and mitigate the threat posed by external entities is crucial to any company or country. There will always be a need for a pragmatic and serious approach to address them through physical security, defensive countermeasures, deterrence, counterintelligence, and reactive investigations. The external entities' TTPs, which are patterns of activities or methods associated with a specific threat actor or group and are the most difficult to decipher according to *The Pyramid of Pain*, have not changed despite the digitization of the modern world. Threat actors of all types (criminals, media, competitive intelligence specialists, dangerous organizations such as terrorist and hate groups, nation-state intelligence officers) all use the same TTPs in both the digital and physical world. They find a vulnerable insider, befriend them, and, when the time is right, make an offer that exploits that friendship.

Author Name, email@address

The factors and stressors that ultimately cause both witting and unwitting insiders to betray their company or country are the same making them prime targets for elicitation, recruitment, and exploitation. In cybersecurity, these stages can happen very rapidly – sometimes in the time it takes an insider to read an email and fall for the trickery of a watering hole attack or installing an attached piece of malware. In the physical world, it may seem slower but the impact, as seen in the documented case studies, is no less devasting.

Though the TTPs have not changed, the world has and will continue to evolve as new technologies are invented and gain accepted use in everyday life. It is crucial for security departments, and specifically InTPs, to concurrently evolve and find solutions that address the root-cause of the problems and not just the symptoms.

References

Allen-Ebrahimian, B. (2018, March 7). *China's Long Arm Reaches into American Campuses*. Retrieved from https://foreignpolicy.com/2018/03/07/chinas-long-arm-reaches-into-american-campuses-chinese-students-scholars-association-university-communist-party/

Aristotle. (350 B.C.E.). *Rhetoric*.

Beyond Identity. (2021). Retrieved from https://www.beyondidentity.com/

Bianca, D. (2014, January 17). *The Pyramid of Pain*. Retrieved from https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Broadkin, J. (2021, March 12). *Apple alleges ex-MacBook Pro Designer leaked Secret Details to Reporter*. ARS Technica. Retrieved from https://arstechnica.com/tech-policy/2021/03/apple-sues-ex-employee-alleging-leaks-of-secret-product-info-to-reporter/

Brook, C. (2020, December 1). *What's the Cost of a Data Breach in 2019*? Retrieved from https://digitalguardian.com/blog/whats-cost-data-breach-2019

Centrify. (2021). Retrieved from https://www.centrify.com/

Charney, D. & Irvin, J. (2016, Spring). The Psychology of Espionage. *Association of Former Intelligence Officers. Journal of U.S. Intelligence Studies*. Retrieved from https://www.afio.com/publications/CHARNEY_and_IRVIN_Psychology_of_Espionage_from_AFIO_INTEL_SPRING2016_Vol22_no1.pdf

Chappel, B. (2013, August 28). *Fort Hood Gunman Nidal Hasan Sentenced to Death for 2009 Attack*. National Public Radio. Retrieved from

https://www.npr.org/sections/thetwo-way/2013/08/28/216512156/fort-hood-gunman-nidal-hasan-sentenced-to-death

Bowie, N. (2020, July 31). *The Face of Chinese Spying in Singapore*. Asia Times. Retrieved from https://asiatimes.com/2020/07/the-face-of-chinese-spying-in-singapore/

Clifton, J. & Harter, J. (2021). *Wellbeing at Work*.

Cohen, Z. (2020, December 9). *Democratic Congressman says he did not share Sensitive Information with Suspected Chinese Spy*. CNN. Retrieved from https://www.cnn.com/2020/12/09/politics/swalwell-targeted-china-spy/index.html

CrowdStrike. (2021). *2021 Global Threat Report*. Retrieved from https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

Department of the Army. (2013). *U.S. Army Counterintelligence Handbook (US Army Survival)*.

Department of Defense. (2017). *Marine Corps Doctrinal Publication (MCWP) 2-6 Counterintelligence*. Compiler. Anderson, T.

Digital Guardian. (2021). Retrieved from https://digitalguardian.com/

Dorfman, Z. (2018, July 27). *How Silicon Valley Became a Den of Spies*. Politico. Retrieved from https://www.politico.com/magazine/story/2018/07/27/silicon-valley-spies-china-russia-219071/

Duntley, J. & Shackelford, T. (2008). *Evolutionary Forensic Psychology: Darwinian Foundations of Crime and Law*.

FBI Internet Crime Complaint Center. (2020). *Internet Crime Report 2020*. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

FireEye Mandiant. (2021). *M-Trends Special Report*. Retrieved from https://content.fireeye.com/m-trends/rpt-m-trends-2021

Forbes. (2020, April 5). *2020 Roundup of Cybersecurity Forecasts and Market Estimates*. Retrieved from https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=733c5e4f381d

Forcepoint. (2021). Retrieved from https://www.forcepoint.com/

ForeScout. (2021). Retrieved from https://www.forescout.com/

Grassley, C. (2020, March 12). *Grassley To Schools: Confucius Institutes Are Fronts For Chinese Propaganda; Just Ask FBI*. Retrieved from https://www.grassley.senate.gov/news/news-releases/grassley-schools-confucius-institutes-are-fronts-chinese-propaganda-just-ask-fbi

Grassley, C. (2018, December 18). *China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses*. U.S. Senate Committee on the Judiciary. Retrieved from https://www.judiciary.senate.gov/meetings/chinas-non-traditional-espionage-against-the-united-states-the-threat-and-potential-policy-responses

Hawkins, A. (2017, February 23). *Alphabet's Waymo Sues Uber for Allegedly Stealing Self-Driving Car Secrets*. Retrieved from https://www.theverge.com/2017/2/23/14719906/google-waymo-uber-self-driving-lawsuit-stolen-technology

Heuer, R. (2019). *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, Central Intelligence Agency.

IBM. (2020). *Cost of a Data Breach Report 2020*. Retrieved from https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542

INSA. (2018). *A Framework for Cyber Indications and Warning*. Retrieved from https://www.insaonline.org/wp-content/uploads/2018/10/INSA-Framework-For-Cyber-Indications-and-Warning.pdf

INSA. (2020). *Human Resources and Insider Threat Mitigation: A Powerful Pairing*. Retrieved from https://www.insaonline.org/wp-content/uploads/2020/09/INSA_InT_Sept252020.pdf

Kantrowitz, Al. (2020, February 19). *How Saudi Arabia Infiltrated Twitter*. Buzzfeed. Retrieved from https://www.buzzfeednews.com/article/alexkantrowitz/how-saudi-arabia-infiltrated-twitter?bfsource=relatedmanual

Knightly, P. (1987). *The Second Oldest Profession: Spies and Spying in the Twentieth Century*.

Knowles, K. (2016, March 22). *Meet the Man Behind FOMO*. Retrieved from https://www.forbes.com/sites/kittyknowles/2016/03/22/fomo-patrick-mcginnis-book-the-10-entrepreneur-fomo-meme/?sh=68c6ef317f1d

Knutson, T. (2020, February 11). *Cybersecurity Jobs Going Begging As College Computer Science Grads Lack Skills/Experience Says House Leader*. Retrieved from https://www.forbes.com/sites/tedknutson/2020/02/11/cybersecurity-jobs-going-begging-as-college-computer-science-grads-lack-skillsexperience-says-house-leader/?sh=565b68b81df1

Lockheed Martin. (2015). *Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense*. Retrieved from

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Lieberman, J. & Collins, S. (2011, February 3). *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*. United States Senate Committee on Homeland Security and Governmental Affairs. Retrieved from https://www.hsgac.senate.gov/imo/media/doc/Fort_Hood/FortHoodReport.pdf

McFadden, C., Nadi. A., & McGee, C. (2018, July 24). *Education or espionage? A Chinese student takes his homework home to China*. Retrieved from https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881

Morgan, S. (2020, August 1). *CISOs Say Security Awareness Training for Employees is Top Priority*. Cybercrime Magazine. Retrieved from https://cybersecurityventures.com/cisos-say-security-awareness-training-for-employees-is-top-priority/

NIST. (2018, December). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Special Publication 800-37. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NITTF. (2018, October 24). *Insider Threat Program Maturity Framework*. Retrieved from https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

Author Name, email@address

NSA. (2013, August 9). *The National Security Agency: Missions, Authorities, Oversight and Partnerships*. Release No: PA-026-18. Retrieved from https://www.nsa.gov/news-features/press-room/Article/1618729/the-national-security-agency-missions-authorities-oversight-and-partnerships

NSA. (2018, March). *NSA's Top Ten Cybersecurity Mitigation Strategies*. Retrieved from https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf?v=1

ObserveIT & ProofPoint. (2020). *The Real Cost of Insider Threats in 2020*. Ponemon Institute Study. Retrieved from https://www.observeit.com/cost-of-insider-threats/

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. (2020, February). *Defense Budget Overview*. Retrieved from https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf

Palo Alto Networks. (n.d.). *What is a Zero Trust Architecture*. Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

Popov, C. (2015, August 30). *Why your Employee Training is a Waste of Time and Money -- And what to do about it*. Forbes. Retrieved from https://www.forbes.com/sites/groupthink/2015/08/30/why-your-employee-training-is-a-waste-of-time-and-money-and-what-to-do-about-it/?sh=7df1795f28cf

Poppe, K. (2018, October). *Nidal Hasan: A Case Study in Lone-Actor Terrorism*. The George Washington University, Program on Extremism.

Author Name, email@address

Ratcliffe, J. (2020, December 3). *China is National Security Threat No. 1*. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/china-is-national-security-threat-no-1-11607019599

Ronel, N. (2011, December). *Criminal Behavior, Criminal Mind: Being Caught in a "Criminal Spin"*. International Journal of Offender Therapy and Comparative Criminology. 55(8): 1208-33.

SANS. (2016, November 5). *504-B Incident Response Cycle: Cheat Sheet*. Retrieved from https://www.sans.org/media/score/504-incident-response-cycle.pdf

Scullard, M. & Baum, D. (2015). *Everything DiSC Manual*.

Sinek, S. (2014). *Leaders Eat Last: Why Some Teams Pull Together and Others Don't*.

Sjouwerman, S. (n.d.). *What is the REAL Cost of Data Breach?* KnowBe4 Security Awareness Training Blog. Retrieved from https://blog.knowbe4.com/what-is-the-real-cost-of-a-data-breach

Smith, J. (2020, January 23). *Pyramid of Pain Vs. The Iceberg of Inspection*. InQuest Labs. Retrieved from https://inquest.net/blog/2020/01/24/Pyramid-of-Pain-Vs-Iceberg-of-Inspection

Smithsonian. (2018). *Inventions: A Visual Encyclopedia*.

State Council, PRC. (2021, May 16). Retrieved from http://english.www.gov.cn/2016special/madeinchina2025/

Stout, M. (2006). *The Sociopath Next Door*.

Swinhoe, D. (2021, January 8). *The 15 Biggest Data Breaches of the 21st Century*. CSO Online. Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Author Name, email@address

Taylor, K. (2020, January 30). *China's Funding of U.S. Researchers Raises Red Flags*. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/chinas-funding-of-u-s-researchers-raises-red-flags-11580428915

Tunggal, A. (2021, March 22). *What is the Cost of a Data Breach in 2021*? Retrieved from https://www.upguard.com/blog/cost-of-data-breach

Tzu, S. (1963). *The Art of War*. Trans. Griffith, B.

U.S. Chamber of Congress. (2017). *Made in China 2025: Global Ambitions Built on Local Protections*. Retrieved from https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

University of Pittsburgh Medical Center. (1971). Mr. Yuk. Retrieved from https://en.wikipedia.org/wiki/Mr._Yuk

United States Code. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text

Van Horne, P, & Riley, J. (2014). *Left of Bang: How the Marine Corps' Combat Hunter Program Can Save Your Life*.

Verizon. (2018). *Data Breach Investigations Report*. Retrieved from https://enterprise.verizon.com/resources/reports/2018-data-breach-investigations-report.pdf

Verizon. (2020). *Data Breach Investigations Report*. Retrieved from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Volkman, E. (2008). *The History of Espionage: The Clandestine World of Surveillance, Spying and Intelligence, from Ancient Times to the Post-9/11 World*.

Author Name, email@address

Walker, L. (2009, July 7). Battered Woman Syndrome. *Psychiatric Times,* Vol. 26, No. 7. Retrieved from https://www.psychiatrictimes.com/view/battered-woman-syndrome

Walker, L. (2016). *The Battered Woman Syndrome*.

Wray, C. (2020, July 6). *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*. Retrieved from https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states

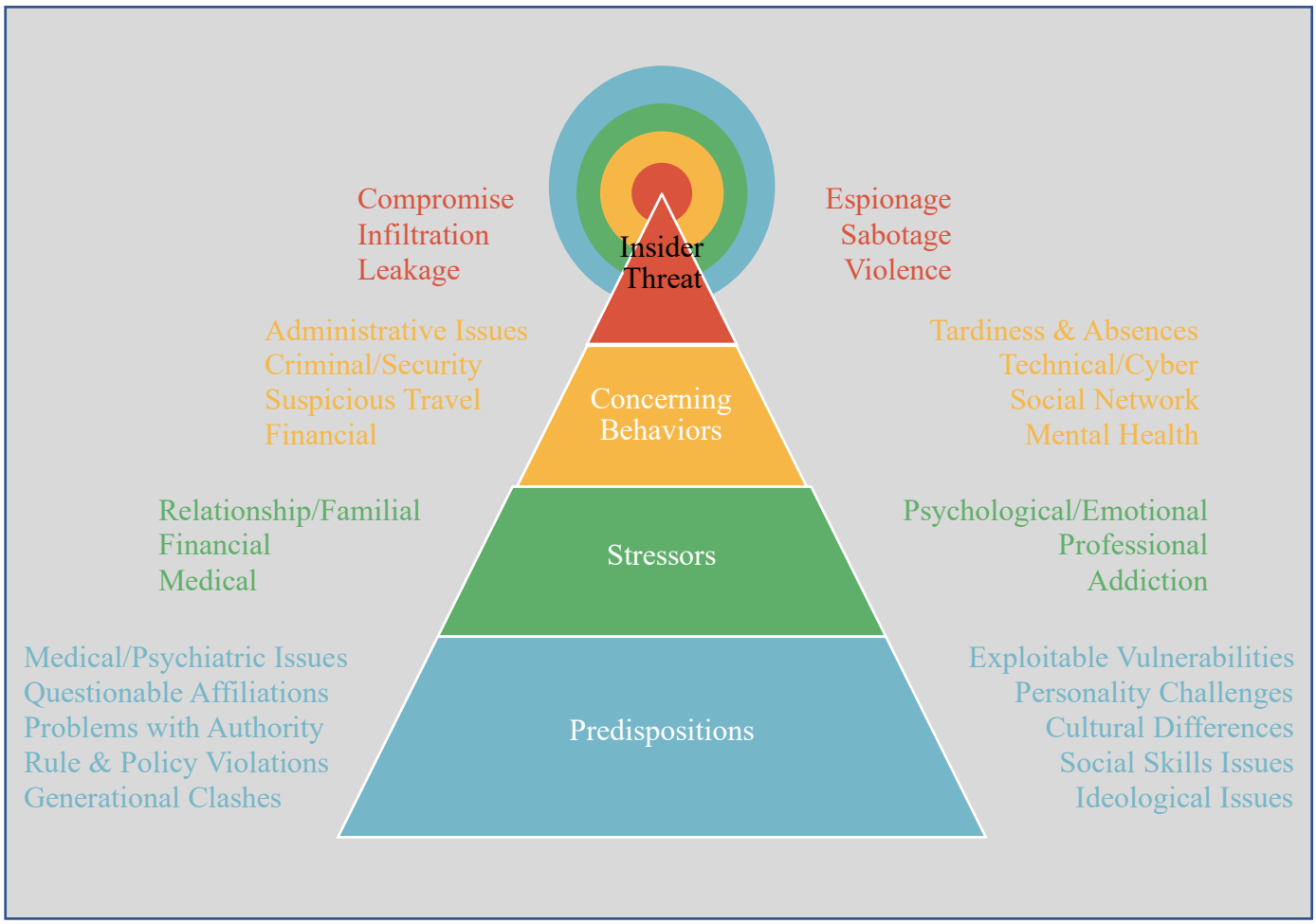
Whiting, J. (2016). *Eight Reasons Women Stay in Abusive Relationships*. Institute for Family Studies. Retrieved from https://ifstudies.org/blog/eight-reasons-women-stay-in-abusive-relationships

Appendix A: Total Revenue (most recently reported via U.S. Securities and Exchange (SEC) Electronic Data Gathering, Analysis, and Retrieval (EDGAR))

Business	Year Company Founded	Total Revenue
A-LIGN HoldCo, LLC	2009	$62,100,000
Code 42 Software, Inc.	2001	$115,000,000
CloudFlare, Inc.	2009	$431,100,000
CrowdStrike Holdings, Inc.	2011	$874,400,000
DarkTrace*	2013	$199,100,000
FireEye, Inc.	2004	$940,584,000
Hack the Box*	2017	$78,300,000
Infoblox, Inc.	1999	$400,000,000
McAfee Corp.	1987	$2,906,000,000
Palo Alto Networks, Inc.	2005	$1,016,900,000
SecureWorks Corp.	1999	$561,034,000
SentinelOne	2013	$122,800,000
Zscaler, Inc.	2007	$431,269,000

*UK companies are not recorded in the SEC EDGAR

Appendix B: Escalation Pyramid of Insider Threats



Author Name, email@address

Appendix C: Open-Source Research and Official Findings on Case Studies

Paige Thompson

- https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-indicted-federal-charges-wire-fraud-and-computer-data-theft
- https://www.nytimes.com/2019/07/30/business/paige-thompson-capital-one-hack.html
- https://www.cnbc.com/2019/07/30/capital-one-hack-allegations-describe-a-rare-insider-threat-case.html
- https://www.businessinsider.com/capital-one-hack-suspect-paige-thompson-shooting-threat-housemate-guns-2019-8
- https://www.wired.com/story/capital-one-hack-credit-card-application-data

Major Nidal Malik Hasan

- https://en.wikipedia.org/wiki/2009_Fort_Hood_shooting
- https://en.wikipedia.org/wiki/Nidal_Hasan
- https://abcnews.go.com/Blotter/fort-hood-warning-signs-missed/story?id=9572844
- https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Nidal%20Hasan.pdf

Ahmad Abouammo and Ali Alzabarah

- https://www.courthousenews.com/ex-twitter-worker-in-saudi-spying-case-released-on-bond/
- https://www.businessinsider.com/twitter-fired-possible-saudi-mole-ali-alzabarah-2018-10
- https://www.justice.gov/usao-ndca/press-release/file/1215976/download
- https://www.bloomberg.com/news/articles/2019-11-21/judge-bets-ex-twitter-employee-arrested-as-saudi-spy-won-t-flee
- https://www.buzzfeednews.com/article/alexkantrowitz/unesco-said-it-wont-renew-a-deal-with-one-of-the-alleged
- https://www.buzzfeednews.com/article/alexkantrowitz/how-saudi-arabia-infiltrated-twitter?bfsource=relatedmanual
- https://www.fbi.gov/wanted/counterintelligence/ali-hamad-a-alzabarah
- https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html
- https://www.justice.gov/usao-ndca/page/file/1232901/download
- https://www.youtube.com/watch?v=joR1eTZmjiI
- https://www.justice.gov/opa/pr/two-former-twitter-employees-and-saudi-national-charged-acting-illegal-agents-saudi-arabia
- https://www.middleeasteye.net/news/ex-twitter-employee-charged-spying-saudis-pleads-not-guilty-23-

charges#:~:text=Abouammo%20was%20arrested%20in%20November,maximum%20sentence%20of%2020%20years.

Chen Jizhong and Zhang Xiaolang

- https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets
- https://www.scribd.com/document/383606662/Complaint-against-Xiaolang-Zhang
- https://www.cnbc.com/2018/07/11/reuters-america-update-3-ex-apple-worker-charged-with-stealing-self-driving-car-trade-secrets.html
- https://www.forbes.com/sites/betsyatkins/2019/02/12/learning-from-apples-spying-incidents-how-to-protect-your-company-from-corporate-espionage/#6674075e6fb4
- https://cdn.ymaws.com/cicentre.com/resource/resmgr/ecoesp_case2/zhang_xiaolang_complaint.pdf
- https://www.youtube.com/watch?v=rh4E1HYFlqc
- https://worldview.stratfor.com/article/arrest-apple-shows-how-corporate-spies-worm-their-way-system
- https://9to5mac.com/2019/02/04/apple-secrets/
- https://www.chinamoneynetwork.com/2019/01/31/second-chinese-national-arrested-in-us-for-theft-of-apples-ip
- https://www.scmp.com/news/china/science/article/2184393/chinese-man-jizhong-chen-stole-apples-future-car-secrets-company
- https://www.bloomberg.com/news/articles/2019-12-09/u-s-says-accused-apple-secrets-thief-had-patriot-missile-file

Liu Ruopeng

- https://en.wikipedia.org/wiki/Liu_Ruopeng
- https://www.forbes.com/profile/liu-ruopeng/#749575cf405b
- https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881
- https://www.businessinsider.com/chinese-billionaire-is-accused-of-stealing-research-from-a-duke-lab-2018-7
- https://cen.acs.org/policy/intellectual-property/Acknowledging-spies-campus/96/i27
- https://en.wikipedia.org/wiki/Kuang-Chi
- http://www.chinanews.com/gn/2012/12-14/4407793.shtml

Unidentified Employee and Egor Kriuchkov

- https://www.teslarati.com/tesla-employee-fbi-thwarts-russian-cybersecurity-attack/
- https://www.justice.gov/opa/pr/russian-national-arrested-conspiracy-introduce-malware-nevada-companys-computer-network
- https://usareally.com/7590-russian-citizen-arrested-and-suspected-of-cyber-sabotage-of-tesla-plant-in-Nevada
- https://twitter.com/elonmusk/status/1299105277485088768?lang=en

Andrew Levandowski

- https://www.newyorker.com/magazine/2013/11/25/auto-correct
- https://www.theverge.com/2019/8/27/20835368/google-uber-engineer-trade-theft-secrets-anthony-levandowski-charged
- https://www.justice.gov/usao-ndca/pr/former-uber-executive-sentenced-18-months-jail-trade-secret-theft-google
- https://www.reuters.com/article/us-uber-tech-volvo-otto/uber-buys-self-driving-truck-startup-otto-teams-with-volvo-idUSKCN10T1TR
- https://www.businessinsider.com/timeline-of-uber-otto-acquisition-2017-2
- https://cdn.ymaws.com/cicentre.com/resource/resmgr/ecoesp_case2/LEVANDOWSKI_Anthony_Order.pdf
- https://cdn.ymaws.com/cicentre.com/resource/resmgr/ecoesp_case2/levandowski_anthony_indictme.pdf
- http://www.reuters.com/article/2012/02/01/us-china-usa-dupont-idUSTRE8100OP20120201

Unidentified USG Employees and Jun Wei Dickson Yeo

- https://www.bbc.com/news/world-asia-53544505?fbclid=IwAR2yx2zf4aUXYaqT8zHLdjQRNfGYJ-gXWzFEh4isMmW8FbBZMMZrIseJpxs
- https://www.justice.gov/opa/pr/singaporean-national-pleads-guilty-acting-united-states-illegal-agent-chinese-intelligence
- https://news-clearancejobs-com.cdn.ampproject.org/c/s/news.clearancejobs.com/2020/07/27/chinese-intel-addicted-to-linkedin/amp/
- https://en.wikipedia.org/wiki/Yeo_Jun_Wei
- https://web.archive.org/web/20180615184809/https://www.reso.rocks/
- https://www.asiaone.com/digital/singaporean-spy-china-schoolmate-reveals-dickson-yeo-sent-him-creepy-fb-message
- https://goodyfeed.com/dickson-yeo-jun-wei/
- https://www.bloomberg.com/news/articles/2020-07-27/singapore-agent-s-ph-d-adviser-says-he-s-glad-ex-student-caught
- https://www.justice.gov/opa/pr/former-cia-officer-sentenced-prison-espionage
- https://www.fbi.gov/video-repository/nevernight-connection-093020.mp4/view
- https://www.fbi.gov/video-repository/nevernight-connection-093020.mp4/view

Jin Julian Xinjiang

- https://www.justice.gov/opa/pr/china-based-executive-us-telecommunications-company-charged-disrupting-video-meetings

Walter Lian-Heen Liew and Robert Maegerle

- https://archives.fbi.gov/archives/sanfrancisco/press-releases/2014/two-individuals-and-company-found-guilty-in-conspiracy-to-sell-trade-secrets-to-chinese-companies
- https://www.topsecretwriters.com/2014/03/first-convictions-under-the-economic-espionage-act-doled-out-and-china-is-involved/
- https://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage
- https://www.bloomberg.com/features/2016-stealing-dupont-white/
- https://archives.fbi.gov/archives/sanfrancisco/press-releases/2014/two-individuals-and-company-found-guilty-in-conspiracy-to-sell-trade-secrets-to-chinese-companies
- https://cicentre.com/resource/resmgr/ecoesp_cases/liew_walter_indictment.pdf
- https://www.justice.gov/opa/press-release/file/1099881/download
- https://www.hoover.org/sites/default/files/research/docs/chineseinfluence_americaninterests_fullreport_web.pdf

Turab Lookman

- https://www.justice.gov/opa/pr/former-employee-los-alamos-national-laboratory-sentenced-probation-making-false-statements
- https://www.sciencemag.org/news/2020/09/former-los-alamos-physicist-gets-probation-failing-disclose-china-ties
- https://www.justice.gov/usao-nm/pr/former-scientist-los-alamos-national-laboratory-pleads-guilty-federal-court-making-false
- https://losalamosreporter.com/2020/09/18/former-lanl-employee-turab-lookman-sentenced-to-five-years-of-probation-and-75000-fine/
- https://www.postandcourier.com/aikenstandard/news/former-los-alamos-worker-pleads-guilty-in-chinese-incentives-case/article_32f94559-3506-5a8f-8719-c5ffb590a4f7.html
- https://www.justice.gov/opa/pr/chinese-national-sentenced-stealing-trade-secrets-worth-1-billion
- https://www.cdse.edu/documents/toolkits-fsos/verbal-elicitation.pdf

Simon Lancaster

- https://appleinsider.com/articles/21/03/11/apple-sues-former-employee-over-device-leaks-to-media
- https://www.theverge.com/2021/3/11/22325827/apple-lawsuit-macbook-designer-simon-lancaster-trade-secrets-leaks
- https://www.ped30.com/2021/03/12/apple-journalist-simon-lancaster/
- https://arstechnica.com/tech-policy/2021/03/apple-sues-ex-employee-alleging-leaks-of-secret-product-info-to-reporter/

Dejan Karabasevic

- http://archive.boston.com/business/articles/2011/09/24/engineer_guilty_in_software_theft/
- https://www.justice.gov/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets
- https://money.cnn.com/2018/03/23/technology/business/american-semiconductor-china-trade/index.html
- https://ir.amsc.com/financial-information/annual-reports
- http://www.sinovel.com/english/content/?113.html
- https://www.forbes.com/companies/sinovel-wind-group/?sh=7fea2c4a32f7
- https://www.wsj.com/articles/china-is-national-security-threat-no-1-11607019599
- https://www.elitetrader.com/et/threads/china-is-national-security-threat-no-1-john-ratcliffe.353324/
- http://www.justice.gov/opa/pr/2013/June/13-crm-730.html
- http://townhall.com/columnists/austinbay/2013/07/17/a-tale-of-two-spy-scandals-n1642341/page/full

Ryan Hernandez

- https://www.justice.gov/usao-wdwa/pr/california-hacker-who-stole-proprietary-information-nintendo-sentenced-three-years
- https://www.infosecurity-magazine.com/news/nintendo-hacker-jailed/
- https://apnews.com/article/technology-child-pornography-california-hacking-palmdale-d9b1479d4bbb2499778f7110c05afdf8

Eric Swalwell

- https://www.axios.com/china-spy-california-politicians-9d2dfb99-f839-4e00-8bd8-59dec0daf589.html
- https://ebcitizen.com/2020/12/09/she-came-out-of-nowhere-then-she-was-gone-the-local-angle-on-swalwells-ties-to-an-alleged-chinese-spy/
- https://www.businessinsider.com/china-suspected-spy-slept-with-mayors-yearslong-intelligence-campaign-axios-2020-12
- https://www.youtube.com/watch?v=SMXcePNFY9M
- https://swalwell.house.gov/media-center/press-releases/swalwell-appointed-serve-intelligence-committee
- https://sanfrancisco.cbslocal.com/2018/08/01/details-chinese-spy-dianne-feinstein-san-francisco/
- https://www.bbc.com/news/world-asia-china-49511231

Appendix D: Elicitation Technique Examples

Technique	Example
Provocative Statement	"I don't think we will ever..."
Quid pro Quo	"I tell you things, you tell me things."
Word Repetition	"You believe you're worked too hard?"
Oblique Reference	"You said 'rugby'. Tell me about it - playing sports is dangerous."
Simple Flattery	"You have worked at the best places…"
Partial Disagreement	"I think your research has a flaw…"
Feigned/Real Disbelief	"I don't believe that you were able to do that."
Reported Facts	"I read on Fox News…"
Naïve Mentality	"I don't really understand what it is that you do."
Confidential Bait	"Just between you and me…"
False Statement	"The Conspiracy Network said…"
Criticism	"That is just a baseless idea."
Instinct to Complain	"You look tired."

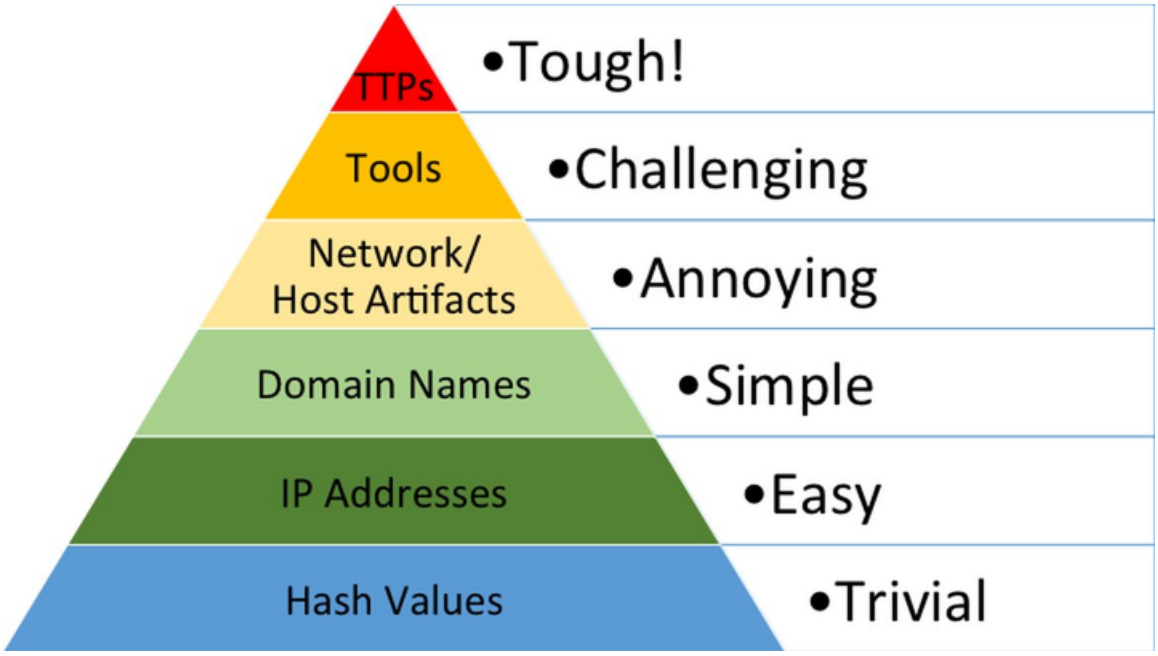
Appendix E: Case Study Summary

Case Study	Manifestation	Motivation of Insider (MICE)	Method of Discovery
Paige Thompson	Leakage	Ego, Disgruntlement	Open source Github discovery
Major Nidal Malik Hasan	Violence	Ideology, Disgruntlement	Internal investigation after attack
Ahmad Abouammo	Infiltration	Financial	FBI referral
Ali Hamad A Alzabarah	Infiltration	Financial	FBI referral
Zhang Xiaolang	Espionage	Ideology	Internal investigation after announcing resignation
Chen Jizhong	Espionage	Ideology	Internal investigation after announcing resignation
Liu Ruopeng	Espionage	Financial, Ideology	Internal investigation after resignation
Unidentified Tesla Employee	Compromise	Financial, Ideology	Self-reported
Andrew Levandowski	Espionage	Financial	Internal investigation after resignation
Unidentified USG Employees	Infiltration	Financial	FBI referral
Kevin Mallory	Espionage	Financial	FBI referral
Jin Julian Xinjiang	Sabotage	Ideology	FBI referral
Walter Lian-Heen Liew	Espionage	Ego, Financial	FBI referral
Robert Maegerle	Espionage	Financial	FBI referral
Turab Lookman	Leakage/ Espionage	Ego	FBI referral
Simon Lancaster	Compromise/ Leakage/ Espionage	Financial, Ego	Internal investigation after resignation
Dejan Karabasevic	Espionage	Financial, Ego	Internal investigation after resignation
Ryan Hernandez	Leakage	Ego	Internal investigation
Eric Swalwell	Infiltration	Coercion	FBI referral

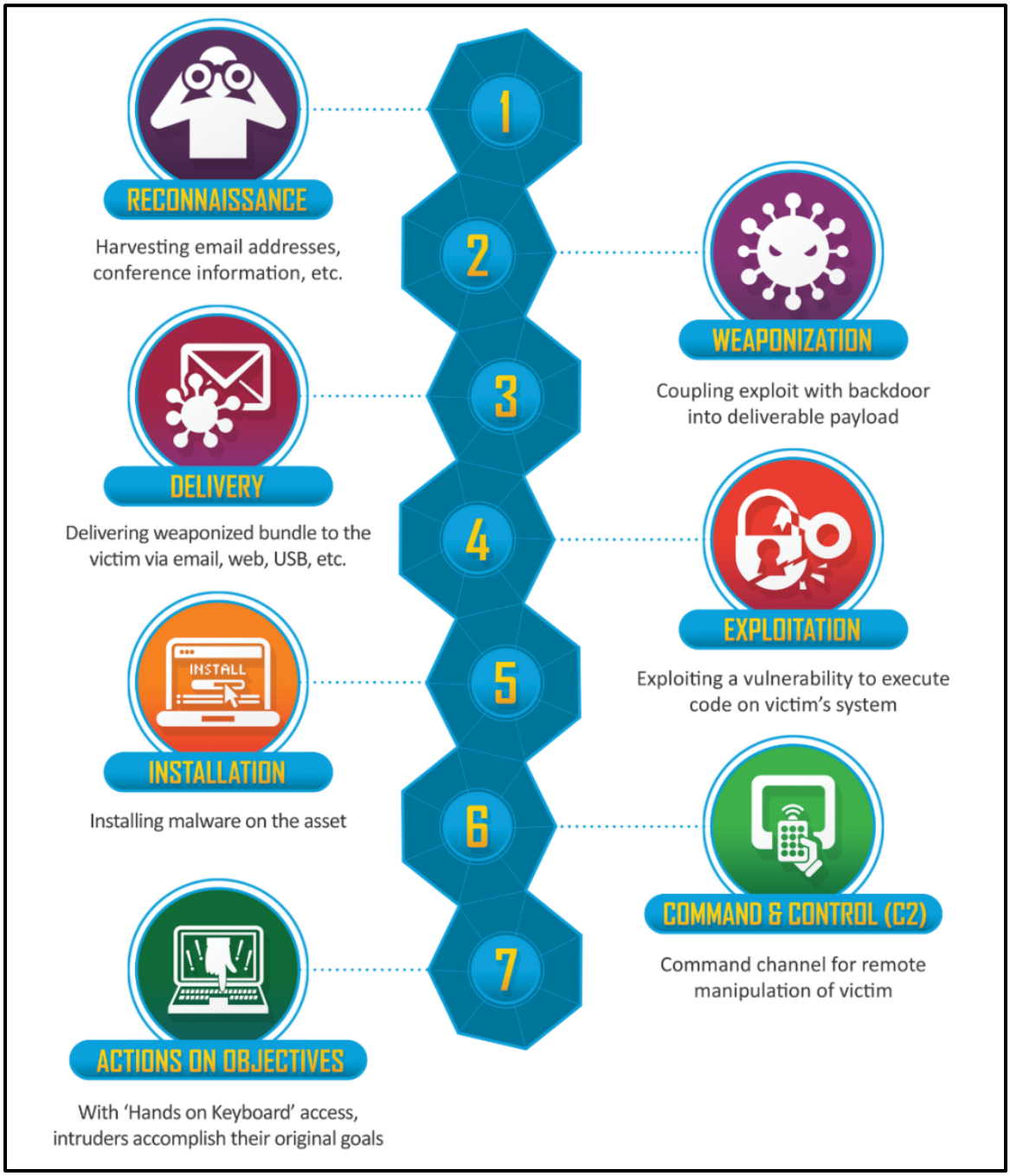
Appendix F: Analysis of Competing Hypotheses

Analysis of Competing Hypotheses (Heuer, 2019)		
1	Hypothesis	Identify all potential hypotheses, preferably using a group of analysts with different perspectives, to brainstorm the possibilities
2	Evidence	List evidence and arguments, including assumptions and logical deductions, for and against each hypothesis
3	Diagnostics	Use a matrix to apply evidence against each hypothesis in an attempt to disprove as many theories as possible
4	Refinement	Review the findings, identify gap, and collect additional evidence needed to refute the remaining hypotheses
5	Inconsistency	Draw tentative conclusions about the relative likelihood of each hypothesis. Less consistency implies a lower likelihood. Eliminate the least consistent hypotheses
6	Sensitivity	Test the conclusions using sensitivity analysis, which weighs how the conclusion would be affected if key evidence or arguments were wrong, misleading, or subject to different interpretations
7	Conclusions and Evaluation	Document and provide the conclusion including alternatives that were rejected

Appendix G: The Pyramid of Pain (Bianco, 2014)



Appendix H: Lockheed Martin Cyber Kill Chain Graphic



Appendix I: Revolutions Per Minute Example (RPM)