The CLOSE PROTECTION & SECURITY JOURNAL

Custodi Civitatem Per Sapientiam!

The Close Protection & Security Journal, Volume 1, Issue 1
Published by the International Protective Security Board - December 2023

Editor-in-Chief Treston Wheat, PhD (Insight Forward)
Editorial Board Members Charles Randolph (Ontic), Fred Burton (Ontic), Charles Tobin (AT-RISK International), Rachael Frost (Frost ICED), and Samantha Newbery, PhD (University of Salford)

The International Protective Security Board is an independent, volunteer organization devoted to promoting the protection industry's interests and professionalization.

Table of Contents

Letter From IPSB President

Elevating the Practice of Close Protection, Security, and Protective Intelligence Through Discourse, Professionalism, and Shared Knowledge

This inaugural launch of a dedicated journal marks a pivotal moment in the evolution of the International Protective Security Board (IPSB) and this dynamic industry. The *Close Protection and Security Journal* (CPSJ) will serve as a platform for sharing ideas and fostering a community where diverse perspectives converge, dialogue flourishes, and collective wisdom illuminates pathways toward enhanced practices and methodologies.

Through its pages, this journal aims to inspire, provoke thought, and catalyze action. It seeks to inform and ignite a spark of inspiration that fuels the continuous evolution of the protection, security, and protective intelligence professions.

As we embark on this journey, let's recognize the inherent potential in exchanging ideas, challenging conventions through discourse, and the relentless pursuit of knowledge. In 1864, poet Robert Browning penned "A Death In The Desert," in which he observed that "Progress" stands as "man's distinctive mark alone." These words echo that the essence of our humanity—our insatiable curiosity, enthusiasm, and drive for advancement—sets us apart. Nowhere is this sense more vividly exemplified than within the Close Protection Industry.

The domains of protection, security, and protective intelligence serve as pivotal elements within our society and industries. They form a crucial shield, safeguarding individuals and organizations against a vast array of threats. The inauguration of the CPSJ is a testament to IPSB's dedication to advancing superior methodologies, questioning established norms, and fostering an environment where innovation and professionalism thrive.

This journal serves as a platform, inviting thought leaders, practitioners, academics, and visionaries to share their insights and expertise, laying the groundwork for a profound evolution in the close protection and security domain. However, its impact hinges entirely on contributions from professionals in the field — your ideas, perspectives, and articles.

The CPSJ has several objectives:

- To provide a platform for the dissemination of high-quality, peer-reviewed research in the field of close protection and security.
- To foster a community of scholars and practitioners who can share ideas and best practices.
- To promote innovation and the development of new and effective close protection and security strategies.
- To elevate the best practices of professionalism in the close protection and security industry.

By providing a platform for the exchange of ideas and the dissemination of knowledge, the *Close Protection and Security Journal* can help to:

- Improve the quality of close protection and security services.
- Develop new and effective strategies for protecting individuals and organizations from threats.
- Raise the bar of professionalism in the industry.
- Attract new talent to the field.

Launching the *Close Protection and Security Journal* is a momentous milestone in the evolution of the IPSB and something I am proud to have been a part of forming. Through it, we will safeguard our community through wisdom, discourse, professionalism, and camaraderie.

Custodi Civitatem Per Sapientiam!

Chuck Randolph
President and Founding Member, **IPSB**

Letter From the Editors

The Mission of Bringing Academic Literature to the Protective Services Industry

Private security has a long history going back centuries, but the focus on creating a close protection and corporate security industry is relatively inchoate, dating back only a few decades. The role of executive protection goes back further, but there was a dearth of cohesion to create a profession with the hallmarks of professionalization and study. To assist this industry's goal of true unity and professionalization, the International Protective Security Board (IPSB) has initiated the *Close Protection and Security Journal* to achieve several purposes.

First, the journal is intended to elevate the study and discussions within the close protection and corporate security communities. Typical discussions within the community focus heavily on tactical situations and personal experiences, and there is often a lack of rigorous study and analysis on such subjects. A significant portion of the security community applies lessons from their personal experiences in law enforcement, military, and government agencies rather than incorporating academic studies or outside disciplines. However, the industry is currently pursuing an elevated conversation on several fronts, especially from various professional associations and conferences. What IPSB hopes to accomplish with the journal is to provide a forum for those kinds of conversations to create industry cohesion.

What do we mean by elevated conversation? That means moving beyond issues like access control, firearms, or vehicles, even though those remain important issues for teams. Rather it means to approach close protection and corporate security as a holistic enterprise in which professionals can discuss systemic approaches rooted in recognized industry and academic best practices and based on multiple disciplines and perspectives. Relatedly, comparable professions to close protection and corporate security went through similar growing pains. Whether it was Sherman Kent developing analytic standards for the CIA or military schools deciding on teaching Clausewitz or Jomini. Close protection and corporate security, in the process of growth, are adapting to such intellectual situations.

Second, the journal creates scholastic literature for the purposes of improved scholarship by both academics and professionals. Preeminent scholar of civil-military relations Samuel Huntington gave three criteria to define a profession: the profession has a function exclusively performed by them, the profession requires formal education and extensive experience, and the profession is self-regulating. Some educational institutions have implemented formal education for corporate intelligence analysis, and there are an increasing number of certification programs for areas like executive protection. As such, this journal is intended to support Huntington's second requirement by helping to create an appropriate literature for the formal education of security professionals.

For those uninitiated into the academic sphere, a subject's "literature" refers to the collection of studies, papers, and scholarship focused on a particular subject. In concert with those studies comes the development of research methodologies and methods along with theories. Corporate security currently operates without these foundations now. That is why the journal has deliberately chosen to be eclectic, allowing interdisciplinary research with mixed methods. Although the journal is eclectic, there is a deep appreciation for case studies because security is intimately tied to the human experience. Purely quantitative approaches based on epistemologies like positivism or systemic theories like behaviorism overlook the human element and the required empathy within security.

Third, the journal assists in the creation of standards for professionalization. Various organizations are attempting to establish standards for professionalization, but there is no current agreement as to what that means. To have standards, the industry will need developed literature based on both quantitative

and qualitative methods. Case-based reasoning, for example, will delineate how protectors have operated in specific situations or how failures took place. Learning from such examples will provide the intellectual basis for creating standards as they show what works and what does not. The quantitative studies shall provide a broad-based analysis of particular principles or issues.

In addition, there is a particularly simplistic approach to much of the training for close protection which lacks standardization for those in corporate security. The absence of modernization can be attributed in part to the scarcity of professional literature. Institutions from which close protection and corporate security draw their inspiration are qualitatively different and are based on long traditions that do not directly apply. Studying tactics are an imperative foundation for protection professionals, but to truly evolve and effectively serve within the profession we must meet the need of maturing a series of modern and soft skills that exist within the day-to-day of close protection.

This inaugural issue brought together scholars, journalists, and practitioners to approach the different problems mentioned above. Importantly, this is just the beginning of the conversation. IPSB's *The Close Protection and Security Journal* welcomes future submissions from all parts of the security field and interdisciplinary research from academics interested in private security. We hope this small contribution will improve the vocation of security for all involved.

Treston Wheat, PhD
Editor-in-Chief, **CPSJ**

Fred Burton
Charles Tobin
Rachael Frost
Samantha Newbery, PhD
Editorial Staff Members, **CPSJ**

Research Articles

Workplace Related Shootings and General Strain Theory

Erin Carling (PhD), Anna Leimberg (PhD), Kirsten England (PhD), Alexis Israel, and Kaylynn Sims

Introduction

Over the last three decades, public mass shootings have occurred in a variety of places and venues. While abundant research has been conducted on school and mass shootings throughout the past twenty years, the academic literature on workplace-related shootings remains scarce, even though these venues are victimized at similar rates (Dillon, 2014; Wheeler, 2016). As the research investigating mass shootings grows and expands, different typologies have been identified to understand these incidents' various forms more effectively. Scholars have generally identified four main mass shooting categories. These include referencing school and workplace settings, terrorism, or those in other public locations specifically where victims were selected for their symbolic value; they do not include schools, education, or workplace settings when the subjects of concern are commonly referred to as "rampage shooters" (Lankford, 2012; Silva and Capellan, 2019).

Often research on mass shootings has tended to describe the "average" perpetrator and case with the exception of school-related shootings, which often draw the most attention, and the scant research hitherto mentioned on workplace shootings. Building off this information, we speculated that more nuances exist regarding venue locations when it comes to the "who, when, where, and why" of mass attacks. While some factors may overlap, such as perpetrators having experienced significant childhood or adult trauma or perpetrators using a mass attack as a "last violent act" in a suicidal crisis, we anticipated those who attack houses of worship likely have different motivations than those who attack schools, government entities, or healthcare settings. Moreover, we opined that perpetrators who engage in roving attacks or work with partners would also exhibit characteristics that stray from the norm.

Literature Review

The typical literature examines specific motivation categories, such as gender-based mass shootings provoked by grievances against women (Silva et al., 2021) and fame-seeking typology and motivation (Lankford & Silver, 2020; Meindl & Ivy, 2017; Larkin, 2009; Silva & Greene-Colozzi, 2020; Bushman, 2018). Other scholars have also investigated the characteristics of completed mass shootings, particularly school-targeted incidents, and foiled or averted or attempted mass shooting incidents (Daniels et al., 2007; Daniels et al., 2010; Agnich, 2015; Langham & Straub, 2019; Silva, 2020; Sallings & Hall, 2019).

While the literature on workplace-related shootings remains seldom, what content is available has revealed traits and characteristics of workplace-related mass shootings and offenders. Peterson and Densley (2019) identify workplace mass shootings as the most common type of mass shooting, with the typical workplace shooter being a male, blue-collar employee, in his 40s, having "trouble at work," and with no specific racial profile. Additionally, other studies suggest that workplace shootings have higher suicide rates, are older in age, use more semi-automatic weapons, and have higher victim fatality rates (Wheeler, 2016; Eisele et al., 1998).

Past studies indicate that the typical offender is a male who acts alone and that these attacks typically end through a use of force by law enforcement, bystanders, or security, or by the offender attempting or

committing suicide (NYPD, 2016). Lankford (2012) compared the main forms of mass shooters that committed suicide and reported workplace suicide shooters make up 43% of the cases identified. These shooters were predominately males and similar in average age to their "terrorists" and "rampage" counterparts (between 37 and 42 years) (Lankford, 2012). Of the suicide mass shooters investigated by Lankford (2012), workplace shooters stood out because their incidents were generally less deadly than the other types, were less likely to have struggled with family problems, were most likely to be linked to a precipitating event (i.e., being fired), and were less likely to provide a statement or note prior to the shooting.

Fox and Levin (1994) similarly identified the "vengeful" employee who resorts to violence as typically a white, middle-aged male who has been fired or is facing termination, particularly in a weakened economy. Silva and Capellan (2019) likewise found that a "disgruntled employee," which they identified as one who targets a current or former workplace as well as those linked to a workplace as partners, owners, and/or investors, tended to be a white male in his late thirties and similar to other mass shooters, except for school shooters who are generally younger.

Since 2000, the evidence regarding active shooter incidents demonstrates compatible increases in the frequency and lethality of these incidents (FBI, 2021a; FBI, 2021b; NYPD, 2016). Both the FBI and NYPD active shooter reports specifically identify workplace-related incidents as making up large shares of their total numbers. Of the 333 incidents identified by the FBI (2021a) from 2000-2019, the category identified as "businesses open to pedestrian traffic" had the highest number of incidents, with 44% of total incidents during this period taking place in areas of commerce, including "businesses open to pedestrian traffic," "businesses closed to pedestrian traffic," and "malls." Consistent with these trends, the NYPD (2016) report found that of the 308 incidents identified between 1966 and 2016, 98 involved some type of professional relationship, noting that "many were perpetrated by individuals who were still employed by the organization at the time of the attack."

While the FBI dataset does not categorize incidents according to the relationship between shooter and victim and cannot distinguish between an act committed by a disgruntled employee in a mall retail store or a violent customer, other scholars have tried to identify this distinction. Martindale and colleagues (2017) identified 105 specific active shooter incidents that occurred at places of business from 2000 to 2015. They distinguished between incidents perpetrated by current/former employees and those by individuals not employed by the business. The authors reported that while the majority of businesses open to pedestrian traffic were attacked by individuals not employed by the business, commercial areas closed to pedestrian traffic were almost exclusively attacked by current or former employees (Martindale, Sandel & Blair, 2017). Consistent with the overall trends identified in the FBI (2021a/b) and NYPD (2016) reports, these business-targeted active shooter incidents were overwhelmingly perpetrated by lone shooters, males, who were white, and with a median age of 41 years (Martindale, Sandel & Blair, 2017). Overall, the authors report that 38% of attackers in business locations were employees or former employees: making up 100% of factory attacks, 55% of office attacks, and 26% of retail attacks (Martindale, Sandel & Blair, 2017).

Particularly noteworthy to the discussion of workplace-related mass shootings are the social and psychological outcomes related to job loss and the threat of losing one's job and work identity. Unemployment and the loss of work are detrimental, beyond a financial burden, to a person's sense of self-worth. This is especially evident in the United States, where work is an important source of identity,

healthcare, social affiliation, and personal meaning (Doherty, 2009; Walsh & Gordon, 2008). Therefore, consequences related to economic downturns like job loss, job insecurity, or a threat to one's work identity can compromise mental health, foster a sense of crippling insecurity, and ultimately have an adverse impact on life satisfaction and subjective well-being (Knabe & Ratzel, 2011; Young, 2012). In turn, this can encourage various destructive, dysfunctional, and violent behaviors such as drug abuse, domestic violence, and suicide (Stack & Wasserman, 2007; Forbes & Krueger, 2019; Riumallo-Herl et al., 2014; Karanikolos et al., 2013; Classen & Dunn, 2012; Renzetti, 2009; Chowdhury, Islam & Lee, 2013).

The anxiety stemming from the threat of job loss can promote negative emotions and drive an individual to act unpredictably, resorting to criminal behavior as a response to the source of their distress. According to Robert Agnew (1992), strain or stress related to a person's job can compel individuals to engage in criminal offending as a reaction to the perceived threat of a negative aspect in their social environment. The General Strain Theory developed by Robert Agnew (1992) asserts that violence is more likely to occur when a goal-oriented individual feels hindrances impeding their aspirations, such as a denied promotion, a poor performance evaluation, a cut in salary, and termination (Agnew & White, 1992; Agnew & Brezina, 2019).

Agnew's (1992) General Strain Theory is based on three different factors: (1) failure to achieve a goal, (2) the existence of harmful impulses, and (3) the removal of positive impulses. The failure to achieve a goal can include monetary success or status in society, the existence of harmful impulses can be family conflict, work conflict, or victimization, and the removal or positive impulses can be financial loss or loss of a romantic partner or family member. Agnew explained that such strain could elevate the likelihood of criminal involvement because it leads to negative emotions such as anger, resentment, and frustration. These negative emotions generate a drive for remedial measures, and engaging in criminal behavior becomes one potential and very common reaction (Agnew, 2006). The possibility of engaging in crime also increases for individuals with poor coping skills and limited resources (Agnew et al., 2002; Cobbs, 2012). Therefore, the General Strain Theory can be used to explain workplace violence as an outcome of individuals' inability to cope with strain in an occupational setting since only a few studies have attempted to understand this relationship fully (Hinduja, 2007; Langton & Piquero, 2007). These studies concluded that those individuals who were discriminated against, harassed, or denied promotions, were all at a significantly higher likelihood to cope through aggressive means.

Novel Contribution of Data

This research extracted information from the Federal Bureau of Investigation's (FBI) active shooter incident (ASI) summaries, which it first published for the years 2000-2013. Since then, the FBI has continued to publish single- or multi-year addendums that include corrections or newly discovered cases for prior years. Altogether the FBI summaries now cover 2000-2022 and served as our basis to build a new U.S. Active Shooter Incidents dataset. In this process, we further expanded our cases and variables collection efforts through document analysis of media articles, news clips, and government bills. To date, our dataset now has 496 cases and 77 variables.

We also adopted the FBI's definition of "active shooter incidents" for our research, which is described in detail within this section. This is an important distinction for the industry to understand as, to date*, there is no federal definition for "mass shootings"* (Booty, et al. 2019). While Everytown for Gun Safety (EGS) utilizes a threshold of four victim deaths by firearm in an event, perpetrator deaths are excluded. On the

other hand, the frequently referenced Gun Violence Archive (GVA) says it excludes assailants from its causality counts, but in reality, the GVA sometimes includes the perpetrator(s) in its case requirement of 4+ individuals in a single event being either wounded or killed by gunshot. Both research projects include incidents that are gang- or drug-related, and EGS also considers shootings that occur in private settings like domestic violence incidents in the home. These case inclusions can be problematic, however, when both private companies and government organizations are seeking to understand the unique phenomena of mass public attacks and how best to prevent them. For example, the definition differences between EGS and GVA have led to EGS reporting only 299 cases from 2009 to 2023 while GVA reports 4,104 mass shootings from 2014 to 2023. (Everytown for Gun Safety 2023, Gun Violence Archive 2022, Booty, et al. 2019). The later project, GVA, is often the one most cited by left-leaning news media to emphasize the need for gun reform and shock the public with the vast number of "mass shootings" that are occurring in the country. However, the general public often does not realize gang-, drug-, and crime-related activities are folded into those numbers, thus causing many to assume a far greater numbers of attacks are occurring that randomly target the public.

In yet another research comparison, Peterson and Densley's "The Violence Project (TVP)" only records 187 mass *public* shootings from 1966 to the present. Like EGS, TVP has a four-victim death threshold for case inclusion, but they confine their cases to public locations and exclude domestic shootings. Following practices similarly utilized by the Federal Bureau of Investigation (FBI), TVP also excludes shootings that are drug-, gang-, or organized-crime related. Peterson and Densley (2019) note this is "not because they are unimportant, but because the perpetrators of these crimes tend to target family members or intimate friends exclusively and have different profiles, motivations, and methods compared with shooters who select their victims more indiscriminately" (p.4). Such distinction is important for private businesses when considering how to best prevent workplace attacks as part of an organization's corporate security plan.

Other research debates continue to arise regarding whether definitional standards should focus on the number of victims *killed* or victims *injured*. Attempting to discriminate between the two, some researchers try to draw distinctions between the terms "mass murder" or "mass killing" for either 3+ or 4+ killed by *one* individual in a public place. Again, though, these definitions do not allow for the inclusion of cases involving multiple attackers or multiple locations (a.k.a., "roving attacks').

In the Investigative Assistance for Violent Crimes Act of 2012, President Obama's administration did set the federal definition for "mass killing" at 3+ victims killed in one incident and gave the FBI authority to oversee such cases. However, neither of these terms specifically denote victim death by firearms. Currently, the closest federal standard on mass shooting incidents comes from a newer definition of "active shooting" set by the FBI (Booty, et al. 2019). The organization sets the standard for an "active shooting incident" (ASI) as "one or more individuals actively engaged in killing or attempting to kill people in a populated area" with the "use of one or more firearms" (Federal Bureau of Investigation 2018, 2). This definition is novel in its allowance for incidents conducted by more than one shooter and/or roving attacks. (Federal Bureau of Investigation n.d.). Our research follows the FBI's definition for "active shooting." The FBI also reports the main venue type where each active shooter incident has occurred: commerce, education, government, open space, residence, houses of worship, health care, and "other". Any of these groups can include multiple locations, but when the venue types vary, those cases have often been listed as "other," "miscellaneous," or "open space" (Federal Bureau of Investigation 2018). With our own research, we use these venue types as a starting point but have corrected the category/categories for each case when document analysis provided new information. We also split the venue categories into subcategories for

deeper comparison and coded individual locations in roving attacks. This process now allows us to comment separately on venue categories, as well as draw comparisons between categories.

Active Shooter Attacks in Retail and Commercial Spaces

The most relevant category for private business in our U.S. Active Shooter Incidents (ASI) is "commercial" venues; other categories include education, healthcare, and houses of worship. "Commercial" venues include various retailers, grocery stores, and variety markets, warehouses, manufacturing companies, freight or delivery business, bars, restaurants, clubs, salons, tattoo parlors, sales and service companies, etc. While ASIs at education venues tend to draw the most media attention, active shootings at the commercial venues are more than 3x's as frequent. Also, while open space ASIs are, on average, the deadliest, if the 2017 Harvest Festival in Las Vegas is excluded from the data, commercial ASIs surpass open space ASIs in average casualties per incident (6.4 to 5.3), average deaths per incident (3.7 to 3.6), and average wounded per incident (2.7 to 1.8). Only the rates for educational venues are higher.

Figure I reports the overall number of ASIs by venue type for the years 2000-2022 and helps highlight the differences in frequency. Attacks on commercial venues occur twice as often as the next most numerous category of open space attacks (i.e., roadways, parks, outdoor political events, festivals, etc.). The fewest shooting attacks occur with houses of worship and healthcare facilities, though each of those categories have their own nuisances regarding the "typical" perpetrator and his or her motives. For example, with houses of worship, attacks by employees are rare. Instead, there is a greater frequency of ideological-based attacks from both left- and right-wing perpetrators.

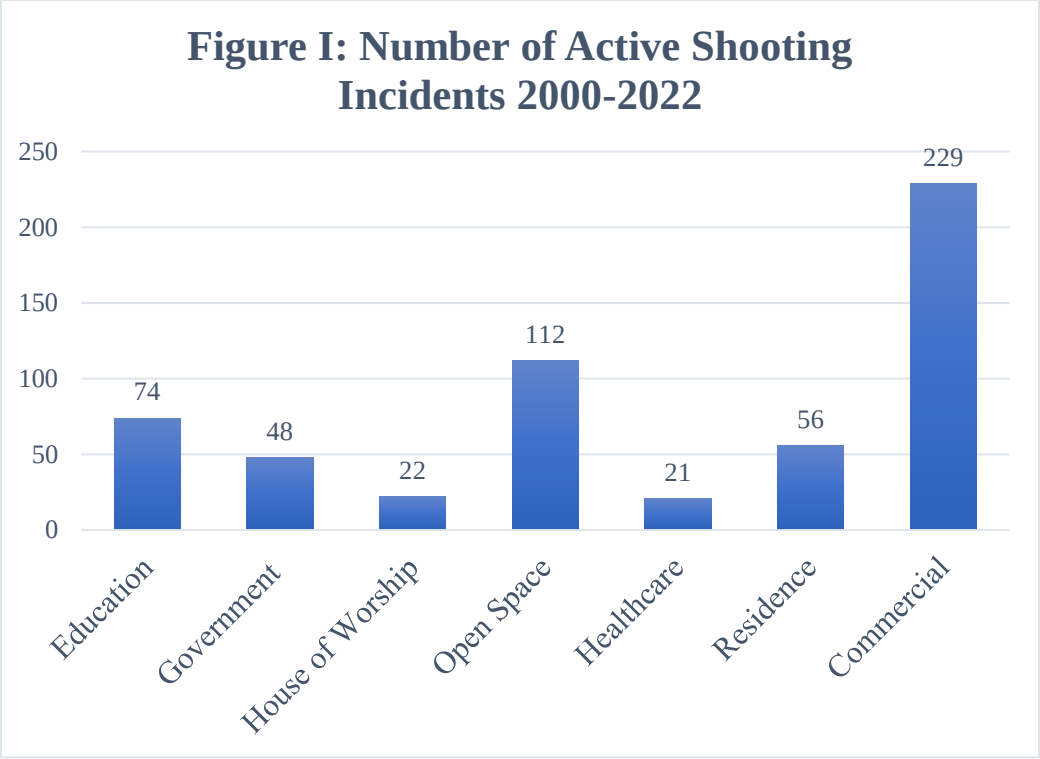
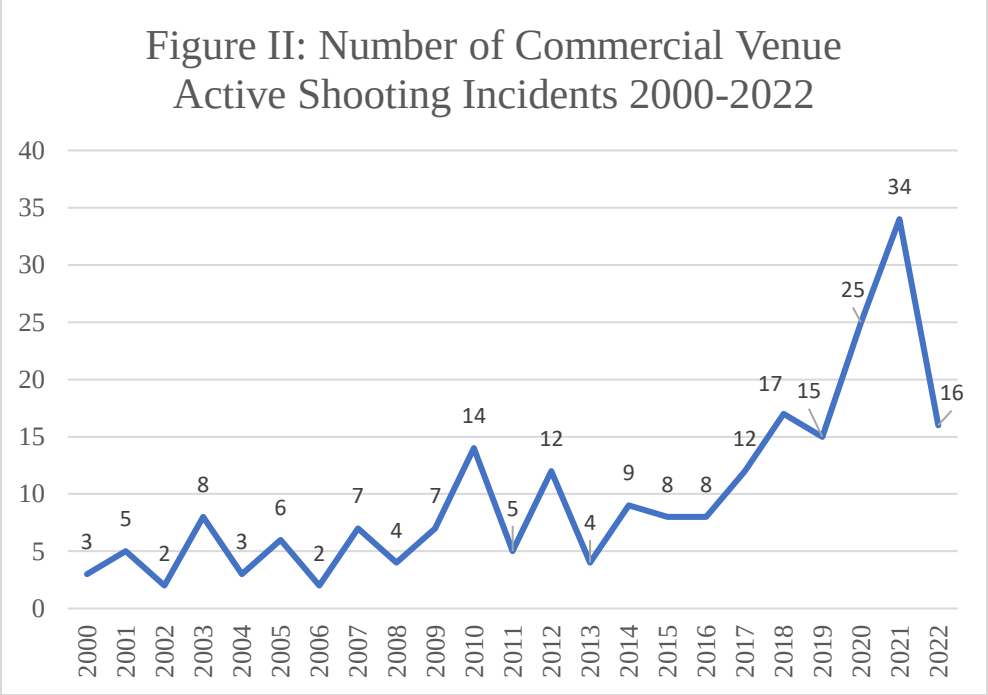


Figure II breaks down the number of incidents by year. Prior to the Covid-19 pandemic, commercial based ASIs had peaked around 14 in 2010 and 17 incidents in 2018. However, 2020 and 2021 saw sharp upticks in the number of incidents to 25 and 34, respectively. Social media posts or writings from ASI perpetrators

in prior years may offer insights on why this phenomenon occurred. For example, in one case, the perpetrator noted schools were not in session, and he did not think he could wait for them to reconvene. Therefore, he needed to turn to alternative targets.

Aside from this, some assailants acknowledged in their writings or confessions to law enforcement that the isolation of the pandemic had greatly increased their loneliness and depression. For others, it had similarly increased their anger towards government overreach and infringement upon personal freedoms. In one 2020 case, a customer placed an order inside the lobby of an Oklahoma City, Oklahoma McDonald's restaurant. After she received her food items, the staff informed the customer that she could not remain inside the restaurant to eat due to Covid-19 restrictions. The disgruntled customer retrieved a gun from her vehicle and returned to fire it at the McDonald's staff. In another case, a perpetrator lamented his increasing loneliness and lack of any romantic relationship. He identified as an "incel" – an involuntary celibate – and blamed the absence of female attention for pushing him towards plotting a mass attack. During his ASI, he targeted both females and couples.



To gain a better understanding of ASIs in commercial spaces and which venues face the most threats, we further subdivided the data into the following 19 subcategories and counted the number of occurrences for each:

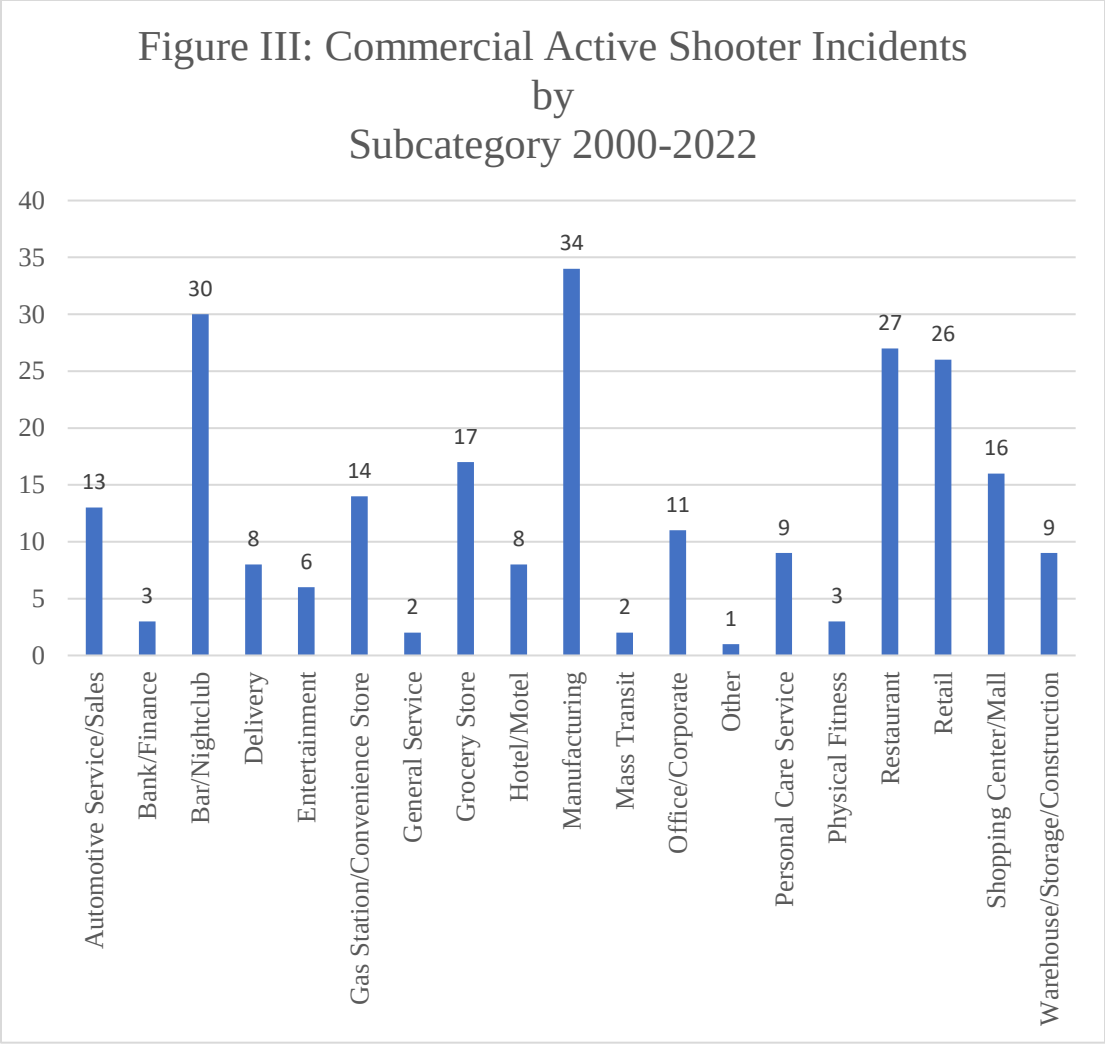
- Automotive Service/Sales
- Bank/Finance
- Bar/Nightclub
- Delivery
- Entertainment

- Gas Station/Convenience Store
- General Service
- Grocery Store
- Hotel/Motel
- Manufacturing
- Mass Transit (for persons; privately owned)
- Office/Corporate
- Other
- Personal Care Service
- Physical Fitness
- Restaurant
- Retail
- Shopping Center/Mall
- Warehouse/Storage/Construction

Figure III compares the number of incidents by subcategory. During those years, manufacturing entities experienced the most ASIs with 34, followed by 30 incidents at bars, pubs, nightclubs, or lounges, 26 incidents at restaurants, and 26 ASIs at retail establishments. Commercial venues were also part of more roving ASIs that any other main category besides open space venues. The frequency with the latter category is to be expected as perpetrators in roving cases tend to either walk or drive from one location to the next, shooting bystanders and intervening officers along the way. Still, 51 of the 229 ASIs on commercial spaces, or 2.3%, were roving in nature. Within these roving cases, the most frequently targeted venues were restaurants (17.6%), gas stations or convenience stores (15.7%), restaurants (15.8%), retail stores (11.8%), and automotive sales or service centers. Together, these three subcategories make up 56.9% of any roving cases related to commercial venues.

This information is important as many roving cases begin with a residential or workplace ASI, after which the assailant fled on foot or by car, often shooting bystanders, law enforcement officers, and nearby vehicles as they travelled. These roving shooters tended to attack restaurants - especially fast-food locations - and retail establishments from the roadway or parking lots. Moreover, gas stations often served as places for assailants to carjack bystanders. The act of changing vehicles or procuring one if the assailant was traveling on foot could briefly prolong the assailant's evasion of police.

Perhaps more so than other locations, these types of commercial establishments are most at risk in roving ASIs and could gain the greatest benefit from lockdown measures at the first alert of shooting incidents in the nearby vicinity, particularly those involving public or domestic targeting. As for what may seem to be an unusually narrow category of "automotive service and sales," 46.2% of ASIs involving these locations were roving in nature. However, that group of cases was evenly split between roving ASIs 1.) beginning at an automotive service center where the perpetrator is a current/recent employee or 2.) simply including the location along the perpetrator's path of attacks.

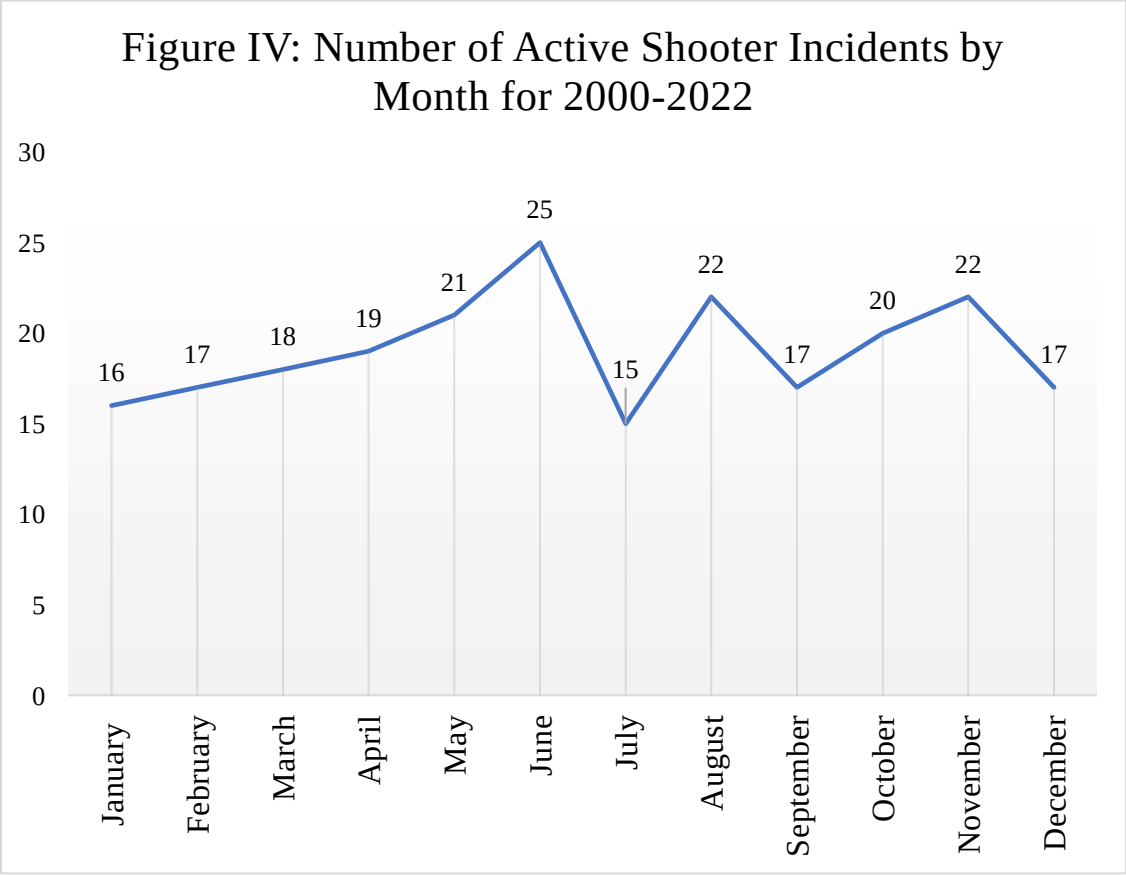


While Peterson and Densley's (2019) research claims active shooters are more often than not blue-collar workers, a clearer connection emerges when one examines the subcategories of commercial venues. 75% of perpetrators in attacks on delivery or freight companies – FedEx, UPS, rail yards, trucking companies, etc. – were current or recent employees. The same is true for 55.6% of perpetrators in attacks on warehouse, storage, or construction companies and at least 35.3% of those who attack grocery stores. However, the most staggering statistics is that 85.3% of active shooters who targeted manufacturing facilities, or 29 of 34 assailants, were all employees at those locations. On the other hand, there are some categories where the vast majority of shooters were not employees. These include bars/pubs, lounges, and nightclubs, as well as gas stations and convenience stores, retail businesses, and most restaurants. With the latter, the great majority of cases involved fast food style places of work.

Other interesting observations to note with these venues is that: 1.) 36.4% of office/corporate attacks involved law offices which were, most often, the legal representation for a party that had opposed the assailant. Many businesses that offered services to the public – from restaurants and grocery or retail stores to hotels/motels and personal care services, etc. – tended to target low- or lower-middle income consumers. Commercial companies could benefit from further research into this connection, but the trend seems to underscore the claim that active shooters tend to target venues or areas that are familiar to them.

Another unusual trend is that more than 1/3 of all active shooter attacks on grocery stores occurred during 2021, and 11 of the 34 attacks on commercial businesses that year were roving in nature. In previous years, the number of roving cases involving commercial venues were, at most, 3 to 5 per year.

To better protect against the potential for mass attacks, some companies have also questioned whether certain times of the day, week, or year are more prone to ASIs. The answer is a bit complex. As Figure IV displays, when adding together all targeted commercial venues from 2000 to 2022, the number of attacks by month range from 15 to 25 with July having the fewest and June having the most. However, the data becomes clearer when seasons are compared. While Spring, Summer, and Fall tend to have close to the same number of incidents – 58, 62, and 59, respectively – there are far fewer ASIs involving commercial venues during the Winter months (only 50). It is also common knowledge amongst researchers on this topic that July 4th and 5th, as well as April 20th – the anniversary of the Columbine massacre – are the dates that experience the most ASIs. However, with all of our 229 commercial venue cases between 2000 and 2022, no incidents occurred on July 4th, only one incident occurred on July 5th, and only two incidents occurred on April 20th. Several other dates were associated with three ASIs over the years. However, only February 12th reached four incidents on a single month-day combination. There may also be some clustering of incidents around November 6th and 7th as each of those days are associated with three commercial venue ASIs.



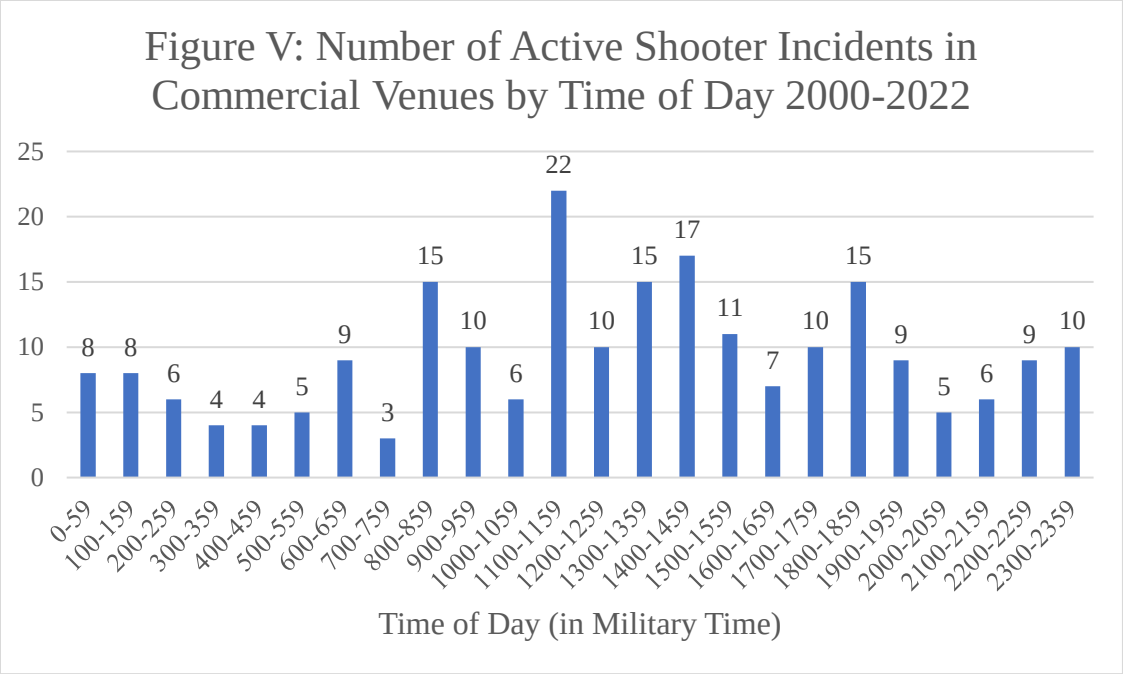
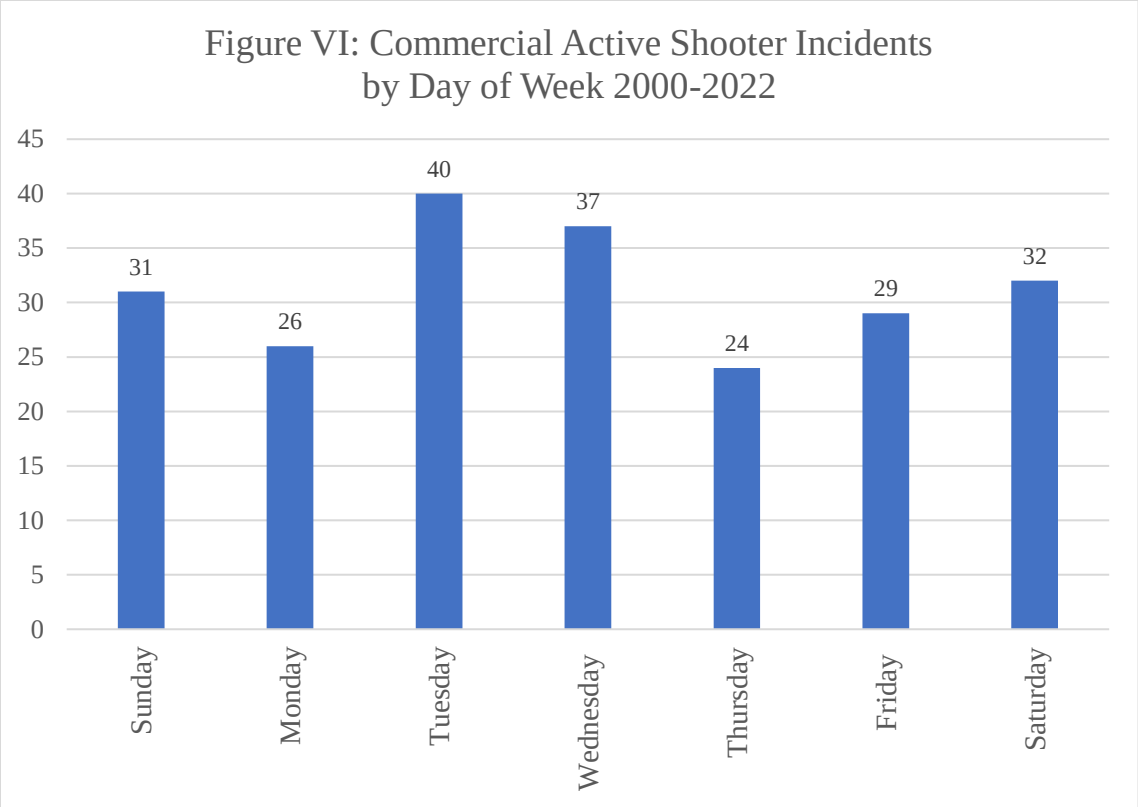


Figure V also displays the frequency of commercial ASIs during hour time windows. The times in the chart are listed in military time. Most interesting is the large spike from 11:00-11:59AM. Within these time windows, bars, pubs, nightclubs, and lounges were popular targets during the late night/early morning hours. From 8:00AM until 9:59AM, blue collar work venues became more frequent targets for commercial venue ASIs. This makes sense as active shooters who have planned attacks may attempt to catch current/former colleagues as they are arriving to work for the day or just as any labor-based place of employment is starting to get going. This time-based phenomenon was also reflected in active shooter attacks on K-12. The lunch time spike from 11:00-11:59AM also combined with the 12:00-12:59PM window of time for an abnormally high number of ASIs that targeted grocery stores and personal care services.

As for days of the week, Thursdays and Mondays tended to have the lowest number of ASIs at commercial venues, 24 and 26 respectively. On the other hand, Tuesdays and Wednesdays experienced the greatest number of commercial-venue ASIs with 40 and 37. While no venue subcategory appearred disproportionate on these days, active shooter attacks at bars and nightclubs, entertainment venues, hotels/motels and even gas stations occurred most commonly on Saturdays and Sundays. On the other hand, very few manufacturing, warehouse, or storage companies experienced ASIs on the weekends. Instead, more than half of the attacks on manufacturing venues occurred on either Tuesday or Thursday. Oddly though, only one ASI event on warehouses, storage facilities, or construction sites occurred on either of these days.



Who Attacks Where and Why?

While many questions form around the logistics of time, date, and location with active shooter incidents in an attempt to heighten company security during the most vulnerable parts of the day, questions also arise regarding the typical profiles of the perpetrators. Again, we argue a different approach should be taken that examines the "typical" active shooter for each venue category and subcategory. Major differences emerge when this is done. For example, almost all attacks on middle schools and high schools are conducted by students. From 2000-2022, only three attacks were carried out by "outsiders" – those who were neither current or former students or teachers with the "former" status being limited to the last year. Within these venues, none of the 34 attacks were carried out by teachers, staff, or administration. On the other hand, of the six attacks that occurred on elementary schools, one was carried out by a recently fired staff member at Pond Gap Elementary in Knoxville, TN who only focused on adult targets in the administrative offices. The other five attacks, however, were all conducted by outsiders, though one was a former student now entering the 9th grade. The student admitted his true issues had been with students at his middle school, and he was unsure why that morning that he had instead targeted his old elementary school (three years removed) other than he wanted to avoid anyone fighting back and simply wanted to create a situation in which the police would kill him as he could not bring himself to suicide.

Within school-based shootings, attackers who are female in sex (not gender) have been almost nonexistent at the K-12 level save for one student who was born as a biological female but identified as a male and acted in tandem with a male or an unidentified 12 year-old student who sought to punish bullies at Rigby Middle School in Idaho. Within commercial spaces, only nine perpetrators were female in sex while 213

were male. We acknowledge that more research remains to be done regarding perpetrators' gender identities. However, we have discovered other important trends regarding the profile of active shooters in commercial spaces.

Sex

Our overall dataset codes basic demographics for 512 active shooters. Across all venues, only 20 were females. Of these, 15 acted alone. The other five acted in coordination with one or two males but never with another female. More interesting, perhaps, is lone attacker female shooters mostly target their places of work – 62% in all venues and 67% in retail/commercial venues. Thus, it is easy to understand why 60% of female shooters in our data were associated with commercial/retail spaces. This percentage is the same for both lone attacker shooters and those who coordinated with others. As for those who acted in conjunction with males, they tended to do so as part of a crime rampage or terrorist attack that was anti-Semitic, racist, anti-government, or Islamist in nature. Also, data regarding the gender identify of active shooters can be difficult to correctly analyze. To date, only a few examples exist of perpetrators that identified as LGBTQ+, and in at least one case, the perpetrator may be insincere with his gender association as many of his ramblings have been misogynistic and some speculate he declared his gender to be non-binary in attempt to further target and ridicule groups he victimized.

Race

Peterson and Densley (2019) noted that the racial breakdown of active shooter perpetrators is somewhat disproportionate to the racial breakdown of the entire United States. They claim African Americans tend to be overrepresented in ASIs by almost the same percentage as whites are underrepresented – 7%. On the other hand, Latino/Hispanic perpetrators are the most underrepresented group when compared to the percent of Latino/Hispanic individuals in the U.S. population. In the 2020 U.S. census, Whites made up 57.8% of the population, down from 63.7% in 2010. However, we find only 47.2% of all active shooters in retail or commercial space attacks from 2000-2022 were White. 18.7% of the U.S. population is Latino or Hispanic, but only 13.9% of perpetrators were. Finally, 36.1% were Black compared to 12.1% of the population.

There were also some special findings to note regarding who targeted what subtype of venues. All ASIs involving entertainment venues – casinos, bowling alleys, theaters – were carried out by White or Latino/Hispanic males. All attacks on physical fitness facilities were also conducted by White males. African Americans were far less prone than other races to attack grocery stores while, on the other hand, only one White person attacked either a hotel or motel.

Age

Overall, the perpetrators in these cases ranged in age from 15 to 79 years-old with 75 of the perpetrators being in their 20s, 56 being in their 30s, 38 in their 40s. Those perpetrators in their teens and 20s conducted the wide majority of attacks on restaurants, bars/nightclubs, shopping centers or malls, and grocery stores. On the other hand, those in their mid- to late-30s and older conducted a wide majority of the attacks on manufacturing facilities, warehouse/storage/construction venues, and office/corporate locations. This may reflect life shifts in what influences individuals to cross the line into becoming active shooters. Often, workers claim depression and thoughts that their life, as they knew it, was over after losing a job and/or going through a divorce. With the latter, divorce or break-up with a partner, especially

in a situation where custody of children is a factor, can be a key reason for assailants targeting the offices of their ex-spouse or ex-partner's legal counsel. Regarding other motivations for engaging in an ASI, individuals of this age were also more likely to note mistreatment at work or feeling like their bosses had wronged them in terms of low pay, work assignments, lack of promotion, or theft of monies the perpetrator felt was owed to him/her for work completed or commission earned.

Lack of Access to Mental Healthcare and Social Benefits

Prior research on strain theory has associated job loss with increases in "deaths of despair" – death by drugs, alcohol, suicide, etc. In addition to this, prior research connects increases in political polarization to less citizen engagement in communal groups, such as religious communities, civic or professional organizations, volunteer groups, etc. When job loss occurs, many workers face losing both mental and physical healthcare benefits. The former can be particularly troubling when individuals face crisis thresholds combined with either a lack of support from communal groups and/or extended family networks, especially as U.S. society continues its shift to concentrating focus only on nuclear families. If there is any lack of a nuclear family, or if the nuclear family breaks down around the same time as when job loss occurs, individuals can turn to extremism or "violent suicide by other means" (i.e., death by police officer or murder-suicide). Thus, going forward, it will be important for the industry to consider how best to address the need to reprimand or fire employees in a manner than minimizes risk and best supports any mental health needs.

Conclusion

The research in this article summarized both available and novel data when it came to ASIs in the workplace and at commercial venues. It explored and delineated the relevant factors, variables, and frequencies that influence such attacks. Furthermore, it looked at how General Strain Theory's three factors of (1) failure to achieve a goal, (2) the existence of harmful impulses, and (3) the removal of positive impulses acts as a catalyst for violence in the workplace and commercial spaces. Scholars have looked at ASIs from a variety of perspectives, but few parts of the literature have really established useful profiles for security practitioners to apply to their work at corporations. The research in this article can be used by those security professionals to inform their risk management and insider threat programs, and corporate security intelligence analysts can use this data to craft profiles for persons of interest. Further research should be done on mitigating factors that close protection and corporate security teams can take, but this article provides a strong basis for that research and other programmatic development within the physical security space.

Authors: Dr. Erin Carlin is an Assistant Professor of National Security Studies with the Institute for National Security and Military Studies at Austin Peay State University. Her research interests focus on crisis management and prevention associated with active shooter incidents, extremism, peace mediation, and corruption.

Dr. Anna Leimberg is currently an Assistant Professor of Criminal Justice in the Department of Criminal Justice at Austin Peay State University. Her research interests include domestic violence, white-collar crime, drug use and other anti-social behavior among youth, and firearm-related violence.

Dr. Kirsten England is an Assistant Professor of Political Science in the Department at the University of South Florida. Her research interests include education policy, gun violence, gun policies, and Constitutional rights.

Alexis Israel is currently an undergraduate student at Austin Peay State University, set to graduate in August of 2024 with a degree in Criminal Justice. Her interests include national security, international terrorism/extremism, and active shooting incidents within schools in America.

Kaylynn Sims is a graduate student from Eastern Illinois University's Political Science Department. Her research interests include race and gender policy, security policy, urban politics and policy, and criminal justice.

Bibliography

Agnew, R. (1992). Foundation for general strain theory of crime and delinquency. *Criminology*, 30(1), 47-88.

Agnew, R. (2006). Pressured into crime: An overview of general strain theory.

Agnew, R., & Brezina, T. (2019). General strain theory. *Handbook on Crime and Deviance*, 145-160.

Agnew, R., & White, H. R. (1992). An empirical test of general strain theory. *Criminology*, *30*(4), 475-500.

Agnew, R., Brezina, T., Wright, J. P., & Cullen, F. T. (2002). Strain, personality traits, and delinquency: Extending general strain theory. *Criminology*, *40*(1), 43-72.

Agnich, L. E. (2015). A comparative analysis of attempted and completed school-based mass murder attacks. *American Journal of Criminal Justice*, 40, 1-22. DOI: 10.1007/s12103-014-9239-5

Bushman, B. J. (2018). Narcissism, fame-seeking, and mass shootings. *American Behavioral Scientist*, 62(2), 229-241. DOI: 10.177/0002764217739660

Chowdhury, A., Islam, I. and Lee, D. (2013). The Great Recession, jobs and social crises: Policies matter. *International Journal of Social Economics*, (40)3, 220-245. https://doi.org/10.1108/03068291311291518

Classen, T. J. & Dunn, R. A. (2012). The effect of job loss and unemployment duration on

Cobbs, J. M. (2012). Empirical test of the general strain theory on workplace shootings.

Daniels, J. A., Buck, I., Croxall, S., Gruber, J., Kime, P. & Govert, H. (2007). A content analysis of news reports of averted school rampages. *Journal of School Violence*. 6(1), 83-89. DOI: 10.1300/J202v06n01_06

Daniels, J. A., Volungis, A., Pshenishny, E., Gandhi, P., Winkler, A., Cramer, D.P. & Bradley, M.C. (2010). A qualitative investigation of averted school shooting rampages. *The Counseling Psychologist*, 38(1), 69-95.

Dillon, L. (2014). *Mass shootings in the United States: An exploratory study of the trends from 1982-2012* (Doctoral dissertation).

Doherty, M. (2009). When the working day is through: The end of work as identity? *Work, Employment, and Society*, 23(1), 84-101. DOI: 10.1177/0950017008099779

Duwe, G. (2016). The patterns and prevalence of mass public shootings in the United States, 1915–2013. *The Wiley Handbook of the Psychology of Mass Shootings*, 20-35.

Eisele, G. R., Watkins, J. P., & Matthews, K. O. (1998). Workplace violence at government sites. *American Journal of Industrial Medicine*, *33*(5), 485-492.

FBI. (2021a). Active Shooter Incidents 20-Year Review, 2000-2019. Accessed from https://www.fbi.gov/file-repository/active-shooter-incidents-20-year-review-2000-2019-060121.pdf/view

FBI. (2021b). Active Shooter Incidents in the United States in 2020. Accessed from https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2020-070121.pdf/view

Forbes, M. K. & Krueger, R. F. (2019). The Great Recession and mental health in the United States. *Clin Psychol Sci*, 7(5),900-913. Doi: 10.1177/2167702619859337

Fox, J. A. & Levin, J. (1994). Firing back: The growing threat of workplace homicide. *The Annals of the American Academy of Political and Social Science*, 536, 16–30.

Hinduja, S. (2007). Work place violence and negative affective responses: A test of Agnew's general strain theory. *Journal of Criminal Justice*, *35*(6), 657-666.

Karanikolos, M., Mladovsky, P., Cylus, J., Thompson, S., Basu, S., Stuckler, D., Mackenbach, J. P. & McKee, M. (2013). Financial crisis, austerity, and health in Europe. *The Lancet*, 381, 1323-1331. http://dx.doi.org/10.1016/S0140-6736(13)60102-6

Knabe, A. & Ratzel, S. (2011). Scarring or scaring? The psychological impact of past unemployment and future unemployment risk. *Economica*, 78(310), 283-293.

Langham, P. & Straub, F. (2019). A comparison of averted and completed school attacks from the Police Foundation Averted School Violence Database. *Office of Community Orientated Policing Services*, U.S. Department of Justice. Accessed from: https://www.policefoundation.org/publication/a-comparison-of-averted-and-completed-school-attacks-from-the-police-foundation-averted-school-violence-database/

Langton, L., & Piquero, N. L. (2007). Can general strain theory explain white-collar crime? A preliminary investigation of the relationship between strain and select white-collar offenses. *Journal of Criminal Justice*, *35*(1), 1-15.

Lankford, A. (2012). A comparative analysis of suicide terrorists and rampage, workplace, and school shooters in the United States From 1990 to 2010. *Homicide Studies*, 17(3), 255-274. DOI: 10.1177/1088767912462033

Lankford, A. (2012). A comparative analysis of suicide terrorists and rampage, workplace, and school shooters in the United States From 1990 to 2010. *Homicide Studies*, 17(3), 255-274. DOI: 10.1177/1088767912462033

Lankford, A. & Silver, J. (2020). Why have public mass shootings become more deadly? Assessing how perpetrators' motives and methods have changed over time. *Criminology and Public Policy*, 19(1), 37-60. DOI: 10.1111/1745-9133.12472

Larkin, R. W. (2009). The Columbine Legacy: Rampage shootings as political acts. *American Behavioral Scientist*, 52(9), 1309-1326. DOI: 10.1177/0002764209332548

Martaindale, M. H., Sandel, W. L. & Blair, J.P. (2017). Active-shooter events in the workplace: Findings and policy implications. *Journal of Business Continuity & Emergency Planning*, 11(1), 1-15.

Meindl, J. N. & Ivy, J.W. (2017). Mass shootings: The role of the media in promoting generalized imitation. *American Journal of Public Health,* 107(3), 368-370. doi:10.2105/AJPH.2016.303611

NYPD. (2016). Active Shooter Recommendations and Analysis for Risk Mitigation. https://www.nyc.gov/assets/nypd/downloads/pdf/counterterrorism/active-shooter-analysis2016.pdf

Peterson, J. K. & Densley, J. A. (November 2019). The Violence Project Database of mass shootings in the United States, 1966-2019. Saint Paul, MN: *The Violence Project*. Retrieved from https://www.theviolenceproject.org

Renzetti, C. M. (2009). Economic stress and domestic violence. *CRVAW Faculty Research Reports and Papers, 1*. https://uknowledge.uky.edu/crvaw_reports/1

Riumallo-Herl, C., Basu, S., Stuckler, D., Courtin, E. & Avendano, M. (2014). Job loss, wealth, and depression during the Great Recession in the USA and Europe. *International Journal of Epidemiology*, 1508-1517. DOI: 10.1093/ije/dyu048

Sallings, R. & Hall, J. C. (2019). Averted targeted school killings from 1900-2016. *Criminal Justice Studies*, 32(3), 222-238. https://doi.org/10.1080/1478601X.2019.1618296

Silva, J. R. (2020). A comparison analysis of foiled and completed mass shootings. *American Journal of Criminal Justice*. https://DOI.org/10.1007/s12103-020-09552-

Silva, J. R. & Capellan, J. A. (2019). A comparative analysis of media coverage of mass public shootings: Examining rampage, disgruntled employee, school, and lone-wolf terrorist shootings in the United States." *Criminal Justice Policy Review*. 30(9): pp.1312-1341. DOI: 10.1177/0887403418786556

Silva, J.R. & Greene-Colozzi. E.A. (2020). Mass shootings and routine activities theory: The impact of motivation, target suitability, and capable guardianship on fatalities and injuries. *Victims & Offenders*. https://doi.org/10.1080/15564886.2020.1823919

Stack, S. & Wasserman, I. (2007). Economic strain and suicide risk: A qualitative analysis. *Suicide and Life-Threatening Behavior*, 37(1), 103-112.

suicide risk in the United States: A new look using mass-layoffs and unemployment duration. *Health Economics,* 21, 338-350. DOI: 10.1002/hec.1719

Walsh, K. & Gordon, J. (2008). Creating an individual work identity. *Human Resource Management Review*, 18(1), 46-61. Http://scholaship.sha.cornell.edu/articles/582

Wheeler, N. A. (2016). Mass shootings and mass media: The discrepancies between workplace and school shootings.

Young, C. (2012). Losing a job: The non-pecuniary cost of unemployment in the United States. *Social Forces*, 91(2), 609-634.

The Growing Importance of Cyberpsychology in Security

David Kirichenko

In his influential masterpiece The Art of War, Sun Tzu cautions against falling for the enemy's lure. This timeless insight holds even greater significance in today's digital landscape. In an era where the tactics of cyber attackers are increasingly intricate, with social engineering at its core, harnessing the capabilities of cyberpsychology will continue to emerge as an essential strategy for protecting both personal and organizational resources. In cybersecurity, we focus predominantly on defense – akin to fortifying a castle. We can harden our systems and have all the right Identity and access management policies in place, but human error can render even the strongest defenses useless. Now this is where the work of cyberpsychology plays a role. Understanding everything that goes on within the people who are fortifying the castle, ensuring they are trained, and human vulnerabilities are well understood to ensure the castle is as secure as possible.

Today's hackers increasingly resort to social engineering techniques, such as baiting or scareware, tapping into human emotions to further their nefarious goals. This fusion of technology and human behavior has created an environment where even top-tier technological safeguards can be negated by preying on human fallibilities. Just 10% of attacks result from vulnerabilities, while 50% stem from credential harvesting, 20% from credential stealing, and 20% from phishing (Saxton, 2023). Social engineering tends to work to deceive individuals to reveal confidential data or grant unauthorized system access. This manipulation is often pivotal for cybercriminals, allowing them to exploit both tech-based and human-centered vulnerabilities. This approach's efficacy is evident, with humans frequently being the Achilles' heel in cybersecurity measures. The continued use and success of phishing and pretexting demonstrate their effectiveness. Their combined use with emerging threats like ransomware is particularly alarming. For example, Verizon's 2023 Data Breach Investigations Report found that "74% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering" (Verizon, 2023).

Hackers often avoid direct confrontations with robust firewalls or challenging antivirus software because it is difficult (Malik, 2023). Instead, they target the most prominent vulnerability present in every network worldwide: humans. Cybercriminals are not merely breaching computer systems; they are trying to manipulate human minds. Phishing attacks, wherein cybercriminals pose as trustworthy entities to gain confidential data or funds, are particularly notorious. The 2016 breach of a private email account linked to Hillary Clinton's presidential campaign, attributed to Russian hackers, resulted from phishing (The Guardian, 2016). A top-ranking Democrat's email account was breached by Russian hackers due to an inadvertent error made by an aide, resulting in Kremlin hackers gaining entry to approximately 60,000 emails stored in the private Gmail account.

In March 2019, the Chief Executive Officer of a UK-based energy company experienced a phone call from an individual who impeccably imitated his superior's voice (Damiani, 2019). The call's authenticity was so persuasive that the CEO mistakenly transferred $243,000 to what was believed to be a legitimate "Hungarian supplier," yet it turned out to be a fraudulent bank account orchestrated by a scammer. It was the first documented scam case utilizing an artificially intelligence-generated deep fake voice (Damiani, 2019). While tech-driven defenses remain crucial, it is vital to address the human aspect of the equation. Drawing from Sun Tzu's wisdom, "To confound the enemy is the essence of strategy.” Therefore, the natural

progression of security after the technical aspects have all been addressed is the human element, and we must use psychology to understand the behavior in the digital or, more preciously, the cyber front.

What is Cyberpsychology?

Cyberpsychology examines the intricate relationship between the digital world and human cognition, assessing how online environments influence our actions in both positive and negative ways (Kashyap, 2018). As technology becomes more integrated into our daily lives—from social interactions to shopping and entertainment—it is essential to understand its profound impact on our thoughts, behavior, and society. Given the digital immersion in our daily activities, our concern with technology's effects on our psyche has grown. Consequently, cyberpsychologists will continue to become more pivotal, offering insights into the juncture of human behavior and technology. Their expertise becomes especially vital as the cyber behavioral sciences see exponential growth, driven by rapid advancements in internet technologies and their deep influence on humans (Maalem Lahcen et al, 2020)

Utilizing psychological principles in cybersecurity allows experts to pinpoint weaknesses in their security programs. Security needs to be designed considering human behavior; it is ineffective if it does not cater to people. The UK's National Cyber Security Centre made an interesting blog post highlighting the pressures on security teams during certain situations. If a high-risk situation arises, like constant attacks from Russia, it may make governments and organizations need to operate at a heightened level (Quallo-Wright, 2022). As a result, this “puts additional pressure on your systems, your processes and your workforce. Cyber security teams were already under mounting pressure in the months leading up to the invasion of Ukraine: handling a global pandemic, a rise in ransomware attacks and the Log4j vulnerability, alongside the usual levels of ongoing malign cyber activity” (Quallo-Wright, 2022). This could result in burnout on the security teams, decrease overall well-being and drive more errors and bad behavior.

Understanding the impact of cyber situations on humans will be crucial to preventing issues in the future. This underscores how the psychology behind the defense is crucial; even the most diligent teams can make errors under stress—a testament to our human vulnerability.

Most common forms of Phishing

Phishing primarily uses deceptive emails as its attack vector, as getting someone to click on an email is far easier than breaking into cyber defenses (Gillis, 2023). These emails cleverly disguise themselves as legitimate messages from trusted entities—an email service, bank, or reputable company. Often, they will falsely claim a need to reset passwords or review important documents. Directed to a fraudulent website resembling the genuine one, unsuspecting recipients are then duped into entering their credentials, granting malicious actors unauthorized access.

Spear phishing refines this technique, crafting messages meticulously tailored for a specific individual (Gillis, 2023). Another variant, 'whaling,' specifically targets high-profile individuals like CEOs or government officials (Gillis, 2023). The personal touch in spear phishing makes it alarmingly effective, significantly increasing the likelihood of the target interacting with the malicious content. Smishing and vishing take similar deceptive approaches, using SMS messages and phone calls (Gillis, 2023). In the case of vishing, con artists might pose as bank representatives, government agents, or technical support personnel.

Or now, with free tools like ChatGPT, crafty users who know how to use prompts creatively can use these methods to make their phishing attempts even more successful. Chatbots have already generated sophisticated phishing emails that appear more convincing and human-like, serving as a foundation for threat actors to insert malware (Adlam, 2023). To more vividly craft how this may happen, a hacker may find the online social media of an employee at one company. Then, they will add all that information and ask ChatGPT to craft a friendly email or send an SMS representing a family member the hacker may have seen in a public Facebook post, for example. ChatGPT could then help craft real messages that will be more convincing to click on.

Introduction of LLMS

Recent advancements in artificial intelligence (AI) have resulted in the development of large language models (LLMs) such as GPT-3, GPT-4, LaMDA, and LLAMA (Lutkevich, 2023). These models excel in producing coherent text passages, writing advanced queries, tackling challenging problems, and even coding. The emergence of LLMs has impacted our day-to-day lives through enhanced chatbots, virtual assistants, advanced content generation, refined search engines, and immersive language learning tools. As AI continues to evolve to simulate human exchanges more authentically, its risk for social engineering will also grow (Adlam, 2023).

While platforms like ChatGPT do have controls over how the technology is used, there is still the vulnerability of "AI Prompt Injection." This flaw arises when adversaries tweak the input or prompt directed to an AI model. We need to give a prompt because it is like a message we give to an AI to tell it what to say or do. It helps control how the AI behaves and the tasks it performs. (Fox, 2023). Such an attack can be executed by overtly influencing the prompt or indirectly, for example, when an AI evaluates content from an external website. Such interferences can cause the AI to yield damaging, deceptive, or unsuitable outputs. Direct injections, in particular, involve an LLM user's direct efforts to deceive the system into divulging unintended information. There is evidence that these threat vectors are already in motion. An April 2023 Darktrace whitepaper reported a staggering 135% surge in unique social engineering attacks across numerous active clients from January to February 2023 (Law, 2023).

People as an attack vector

In the realm of cybersecurity, humans remain the most exploited attack vector. While technology can be refined and enhanced to create stronger defenses, human vulnerabilities often remain a consistent challenge. Simply put, no matter how sophisticated our systems become, they are operated by people prone to mistakes, manipulation, or simple oversights. This is why it is crucial to recognize and address the human element when designing security measures. Often, security breaches are not the result of cutting-edge hacking techniques but rather exploiting common human errors or lapses in judgment. Phishing emails, for instance, prey on such human vulnerabilities, enticing individuals to click on malicious links or share sensitive information.

Grasping the behavioral economics that dictate individuals' evaluations of risk and reward, especially considering certain cognitive limitations, is essential. Additionally, it is crucial to pinpoint situations where individuals might be more inclined to overlook the risks of divulging private information. For instance, research has shown that individuals share more personal and sensitive details in relaxed environments, like informal chats or social media platforms (Leslie, John, Acquisti A, Loewenstein G, 2023).

Adversaries are adept at manipulating human emotions like anxiety, greed, curiosity, and a sense of urgency to uncover weak points. Crafted emails with tailored details—such as the recipient's name, profession, interests, or prior projects—significantly enhance the likelihood of the email's links or attachments being accessed. Ensuring email content is contextually pertinent to the recipient is vital; referencing a familiar corporate event or project can imbue the sender with credibility. Masquerading as a known associate or peer greatly escalates the chances of ensnaring someone with a spear phishing tactic. The capacity to leverage human emotions remains a potent weapon for attackers.

It is possible to exploit even the savviest users by using psychology. To prevent this, companies must also invest in understanding the cyberpsychology of their workforce. People do not generally come to work and look for ways to introduce errors into what they are doing. They are simply overwhelmed, and processes break down, and that's when mistakes happen (Saxton, 2023). This loud, always-on environment creates the leading cause of poor performance levels: cognitive overload. Cybersecurity analysts are faced with too many tasks, and too much information to properly do their jobs – and the mental stressors behind these challenges are often the critical catalyst for missed red flags and careless practices.

Who is most at risk?

In the digital world, everyone is vulnerable, largely due to our innate tendency to trust rather than question. Cybercriminals capitalize on this trust, employing tactics inspired by renowned US psychologist Robert B. Cialdini's six principles of persuasion: Reciprocity, Scarcity, Authority, Commitment and Consistency, Consensus/Social Proof, and Liking (Maurer, 2023). They merge these principles with the 'big five' personality traits: Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism.

Take, for instance, an individual who frequently posts public selfies on social media. Upon seeing these posts, cybercriminals might deduce the individual to be extroverted or even narcissistic. This understanding becomes especially valuable when the target holds a significant position. Imagine a professor; a simple phishing email titled "You've been quoted" with a deceptive link could be the trap (Maurer, 2023). The prevalence of narcissism can be a potent tool, often acting as the "master switch."

Continuous training can diminish the success rate of phishing attacks by 20 to 80% (Maurer, 2023). The most enduring impact comes from prolonged security campaigns. Employees often exhibit progress even after several sessions. Yet, the scope of cybersecurity is vast, leaving room for many potential missteps. It is essential to assess skills and knowledge before training begins. Based on these assessments, one can develop tailored course clusters. The training structure is equally crucial, a domain where cyberpsychology offers insights. Understanding how to motivate individuals and incorporating gamification for engaging lessons can make training sessions more effective. The ultimate goal is to instill a behavioral change in employees, making security precautions an instinctive part of their routines (Pratt, 2023).

How the U.S. government is thinking about cyberpsychology

Cyberattacks have become an escalating concern for individuals, businesses, and governments as hackers exploit human vulnerabilities for personal gain. Despite safeguards like firewalls, anti-virus software, and multi-factor authentication, the inherently human-focused tactics of advanced attacks remain challenging to mitigate. Addressing this, the Intelligence Advanced Research Projects Activity (IARPA) has unveiled its latest initiative, Reimagining Security with Cyberpsychology-Informed Network Defenses (ReSCIND). This

innovative strategy incorporates cyberpsychology, a field bridging human behavior and the digital realm, into defensive frameworks.

In contrast to traditional, reactive cybersecurity measures, ReSCIND proactively seeks to leverage the cognitive vulnerabilities of cyberattackers (Mariah, 2023). The program's design aims to impose "costs" on these attackers through wasted time and resources, aiming to delay or even prevent cyber threats, thereby reshaping the landscape of cyber defense. Kimberly Ferguson-Walter, ReSCIND's Program Manager, champions the potential impact of these cyber penalties in repelling attacks (Mariah, 2023). Drawing on past experiments using decoys - fictitious entities meant to mislead and detect invaders - she noted their efficacy even against veteran hackers. Such decoys hampered attacker momentum and signaled their intrusion, underscoring the power of manipulating cognitive biases in cybersecurity.

Conclusion

Humans frequently become the most vulnerable component when dealing with security systems. Our inherent behavioral patterns and cognitive boundaries render us prone to online deceptions. However, it is essential to recognize that many cyber attackers are human. Discerning their psychological tendencies and vulnerabilities can offer a strategic advantage.

Having a cyberpsychologist onboard to advise can give teams a broader perspective, allowing them to see the bigger picture while understanding their adversaries. With cybersecurity threats intensifying, it is clear that today's threat actors are more cunning than ever. However, the tools to counter these threats have also evolved in sophistication. Cyberpsychology is not merely a trendy term; it is a tangible method for designing systems that acknowledge human fallibility and cognitive limitations. By investing in this discipline, organizations can anticipate and preempt malicious attacks, ultimately improving their overall security posture. Incorporating cyberpsychology into defense strategies acknowledges our human frailties. While some cybersecurity measures, such as honeypots, are already exploiting these human tendencies in attackers, fully integrating cyberpsychology into defensive blueprints remains a largely untapped strategy.

Author: David Kirichenko is a security practitioner with experience in cloud security and vulnerability management. His analysis and writing are published widely in publications such as the Center for European Policy Analysis, Atlantic Council, The Hill, and the Irregular Warfare Center, as well as peer-reviewed journals.

Works Cited:

"2023 Data Breach Investigations Report." Verizon Business. 2023. https://www.verizon.com/business/resources/reports/dbir/.

Adlam, Stephanie. "CHATGPT Has Become a New Tool for Cybercriminals in Social Engineering." Gridinsoft Blog, June 6, 2023. https://gridinsoft.com/blogs/chat-gpt-social-engineering/.

"Cost of a Data Breach 2023." IBM, 2023. https://www.ibm.com/reports/data-breach.

Damiani, Jesse. "A Voice Deepfake Was Used to Scam a CEO out of $243,000." Forbes, September 3,2019.https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=2481c62b2241.

Fox, Jacob. “Prompt Injection Attacks: A New Frontier in Cybersecurity.” Cobalt, July 31, 2023. https://www.cobalt.io/blog/prompt-injection-attacks.

Gillis, Alexander S. “What Is Phishing and How Does It Work?: Definition from TechTarget.” Security, June 21, 2023. https://www.techtarget.com/searchsecurity/definition/phishing.

Irvin, Mariah. “Using Psychology to Rescind Cyberattacks.” IARPA, March 27, 2023. https://www.iarpa.gov/newsroom/article/using-psychology-to-rescind-cyberattacks.

Kashyap, Naveen. “Lee Hadlington, Cybercognition: Brain, Behaviour, and the Digital World.” Psychology Learning & Teaching 17, no. 3 (2018): 323–25. https://doi.org/10.1177/1475725718787921.

Law, Marus. “Scam Email Cyber Attacks Increase after Rise of Chatgpt.” Technology Magazine, April 3, 2023. https://technologymagazine.com/articles/scam-email-cyber-attacks-increase-after-rise-of-chatgpt.

Leslie, John, Acquisti A, Loewenstein G. Strangers on a plane: context-dependent willingness to divulge sensitive information. Journal of Consumer Research 2011; 37(5): 858–873.

Lutkevich, Ben. “12 of the Best Large Language Models.” WhatIs.com, July 14, 2023. https://www.techtarget.com/whatis/feature/12-of-the-best-large-language-models.

Maalem Lahcen, Rachid Ait, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. “Review and Insight on the Behavioral Aspects of Cybersecurity.” Cybersecurity 3, no. 1 (2020). https://doi.org/10.1186/s42400-020-00050-w.

Malik, Keshav. “Are Humans the Weakest Link in Cyber Security?” Astra Security Blog, January 16, 2023. https://www.getastra.com/blog/security-audit/humans-in-cyber-security/.

Maurer, Stefan. “Cyberpsychology – Employees as the Key to IT Security.” bechtle.com, January 23, 2023. https://www.bechtle.com/de-en/about-bechtle/newsroom/new-horizons/2023/cyberpsychology-employees-as-the-key-to-it-security.

Pratt, Mary. “Why Cyberpsychology Is Such an Important Part of Effective Cybersecurity.” CSO Online, July 4, 2023. https://www.csoonline.com/article/643967/why-cyberpsychology-is-such-an-important-part-of-effective-cybersecurity.html.

“Top Democrat’s Emails Hacked by Russia after Aide Made Typo, Investigation Finds.” The Guardian, December 14, 2016. https://www.theguardian.com/us-news/2016/dec-14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds.

Quallo-Wright, Marsha. “Preparing for the Long Haul: The Cyber Threat from Russia.” NCSC, July 5, 2022. https://www.ncsc.gov.uk/blog-post/preparing-the-long-haul-the-cyber-threat-from-russia.

Saxton, Mike. “Three Ways to Leverage Cyberpsychology to Prevent Attacks.” SC Media, May 7, 2023. https://www.scmagazine.com/perspective/three-ways-to-leverage-cyberpsychology-to-prevent-attacks.

Red Teaming: Program Development Through a Case Study

Shawn Abelson and Ana Aslanishvili

Industrial Espionage Case Study

The Defender's Perspective (Shawn)

I watched the camera feed helplessly from my desk 150 miles away, as an intruder broke into a secure research and development facility. They followed the signs for the "high security zone" that contained more than a billion dollars' worth of sensitive medical device research that I was tasked with protecting. It felt like a TV show as I waited for the dramatic chase scene and arrest of the criminal. Unluckily for me and unlike TV, this was unfolding in real time and was really happening.

The intruder rounded a corner and followed three strides behind a researcher as they swiped a badge to enter the "high security zone." This was the center of the secured office building, and it contained labs and equipment needed to develop, prototype, and manufacture proprietary medical technology. Now that the researcher and the intruder were both inside, the intruder quickly looked at their phone and stood awkwardly with an unknown object in their hand as they walked away from the busy lab desks, down a hall, and out of range for the limited cameras in the area. The researchers nearby did not look up and were blissfully unaware of the fox they just allowed to tailgate into the hen house.

On the edge of my seat, I continued hoping for a large contingent of security officers to arrive and stop the intruder. Instead, four minutes later, I saw the intruder pop up on cameras again as they loaded research papers and prototypes into a large box. As I lost all hope, I noticed a researcher in the lab begin talking to - and hopefully confronting - the unknown person packing a box to remove prototypes from a space, doing so sandwiched between two signs that said, "Removing prototypes from this area is strictly forbidden." As they spoke, I was grateful and excited that one member of this high security lab had the awareness to confront an unknown and unbadged stranger.

In a moment all too familiar to security professionals, I watched in shock as the researcher picked up the box of prototypes and began walking out of the building next to the adversary, helping to load the packed items into an SUV backed into the parking spot just outside of the emergency exit. Multiple prototypes walked straight out of the high security area, outside of the secured building, right into a stranger's car - and it was an employee, not the intruder, who carried the box.

The Attacker's Perspective (Ana)

It was a seemingly typical day at the innovation business park with employees and visitors moving about the main office building that I planned to work in that day. As I walked across the parking lot, I saw familiar faces of employees who worked in the labs. I scrolled through my phone as I followed through a side entrance behind a researcher, glancing at the building's emergency map as I thanked him for holding the door for me. Once inside I turned left down a long hallway and made my way towards my destination, the high-security lab area. No time for chatting; it was a busy day, and I had a few things to accomplish before I could leave the campus. I poked my head into the research lab and then kept walking through the workplace until I was at my destination. It was lunchtime and I kept throwing glances over to my bag of

pistachios as I started to pack a bright red storage bin full of what appeared to be sensitive, confidential R&D hardware parts and prototypes.

This was my last task of the morning. After this bin was secured in my vehicle I could relax and have lunch after a stressful morning. A researcher I have not yet met emerged from the lab, and I noticed that he was wearing a t-shirt with my favorite band on it. Without hesitation I complimented the shirt and his taste in music, and we started chatting. After learning about his research, his morning, and his favorite local place to get lunch, I grabbed my coveted bag of pistachios, and we walked out together through multiple sets of doors as he helped carry the heavy red container. I clutched my pistachios and held the doors open for him. We loaded my car with the prototypes I was asked to pick up, I thanked him, and I left the parking lot with pistachios on the dash.

Not a week later, I was asked to join an important call at work. A large team of subject matter experts were gathered to discuss the known details and implications of a breach that happened days prior. There was security footage from CCTV cameras, an internal investigation, and many questions about what enabled a perpetrator to walk away with more than a billion dollars' worth of sensitive technology without so much as setting off an alarm or receiving a report of suspicious activity. Every head in the room turned to look at me. I did not have all of the answers, but I did have some. I grabbed a bag of pistachios from my desk, removed the hidden camera inside it, and plugged it in to share the footage and the tale of this particular red team operation.

What is a Red Team?

A red team exists to test and improve important systems.

A red team is a group of professionals who conduct pressure-tests of important systems, decisions, or technologies to identify weaknesses and aid decision-makers in improving defenses. The Center for Advanced Red Teaming (CART) at the University of Albany defines Red Teaming as "Any activities involving the simulation of adversary or adversarial decisions or behaviors, where outputs are measured and utilized for the purpose of informing or improving defensive capabilities." As the most advanced tool in a security team's toolbelt, red teams are mission-driven to test and improve any organization's security by soliciting an organic, realistic response to varying aspects of security testing.

Red team operations are commonly conducted in both private and public sectors. Their goal is to test the defenses of an organization before a real criminal does. In simple terms, red teams pretend to be criminals trying to steal a company's valuable information or assets to test if its security systems work in general and sometimes if they work as designed. If a red team succeeds in breaking through systems, valuable evidence is provided to whoever oversees the systems so they can fix any issues before a real criminal can also succeed in leveraging them for malicious intent. Red teams routinely find major issues and help fix them proactively. On the other hand, if a real criminal breaks through the defenses, the result can be catastrophic breaches with the financial, reputational, regulatory, privacy, and legal implications that follow.

What sets red teams apart from vulnerability scans and bug hunters are psychology, perspective, prioritization, and approach. Instead of identifying all vulnerabilities, a good red team seeks to understand and emulate the most serious adversaries and tests the systems or layers of security which are most likely to be targeted and that have the greatest overall impact on a business. Red teaming is not automated,

instead using the team's expertise in combination with several methodologies, such as alternative analysis and threat modeling, to prioritize assessment specifics based on threats facing the target. The goals of a red team can be viewed below:

Support the Business's Ability to Profit and Operation without Interruptions

↓

Improve the Business's security and resilience

↓

Test security and resilience measures

Red Teams exist to test and improve important systems. These may include assessments of cybersecurity or physical security programs, or systemic improvement of decisions, intelligence estimates, and military planning for defense organizations across the globe. The scopes and roles of red teams vary significantly across the industry. As an increasingly important subsection of the red team community, physical security red teaming still has relatively few dedicated frameworks, resources, or organizing bodies to support the profession. This review defines physical security red teams as any red team with the role of testing a physical security entity. Cybersecurity red teams may have the responsibility of also testing physical security at an organization and would meet the definition of a physical security red team. It should be noted that physical security red teams are not limited to only conducting physical security penetration tests. Their responsibility is to test and improve the entire physical security organization, which often also includes crisis management, intelligence, vendor management, and many other domains. Red teams are advanced multi-dimensional audit teams, aiming to test various security functions before a real incident or adversary does.

Defining Red Teaming Across Industries

It is reductive to write only about security-focused red teaming when the concept of a devil's advocate or pressure-testing team has spread across companies, sectors, and governments to address some of the biggest issues facing society today, with many outside of the security space entirely. Red teams exist across many spaces, including Artificial Intelligence (AI), Trust & Safety, Technology, Cyber, Hardware, Software, Military, Intelligence, and Physical Security.

Many companies and governments with high-value assets requiring protection have cybersecurity or physical security red teams. As the concept of red teaming has grown, new types of red teams have started to emerge. These red teams operate in new domains, unrelated to traditional security and penetration testing.

These newer red teams can test and improve modern day systems such as Trust & Safety systems (i.e., content moderation of social media sites), AI algorithms, and the red teaming of significant decisions that business, military, and government leaders must make. Remember, red teams exist to test and improve important systems. Those systems may involve company leadership making major decisions about the direction of the company, or AI engineers trying to understand how their algorithms could be misused. No formal taxonomy exists to track the various types of red teams; however, they can be broadly categorized as follows:

- Critical System Testing (CST) - Testing a System
- Applied Critical Thinking (ACT) - Challenging How We Think or Decide

Within Critical Systems Testing, there are many different red teams types and approaches:

- Critical Systems Testing (CST)
    - Security
    - Physical Security
    - Cyber Security
    - Hardware
    - Software/Systems
- Belonging to Company
- Belonging to Vendors (i.e., mitigating 3rd-party risk)
    - Privacy & Information Security
    - Algorithms
    - Content Moderation
    - AI Systems

Applied Critical Thinking is a cognitive assessment method of purposely changing one's perspective to see a problem from different perspectives. Contrarian thinking is not simply taking an obstructionist view of a problem or issue. Rather, it is a systematic approach in which core assumptions and/or formal logic of a process or decision are challenged to ensure they represent the most appropriate mode of analysis for the given problem set or circumstance.

Within Applied Critical Thinking, the use of red teams is typically either systemic or ad-hoc. Systemic means that the red teaming is part of an ongoing organizational process (e.g., the intelligence lifecycle) that provides their services on a regular basis. Systemic red teams are often in-house red teams made up of company employees dedicated to their red team role. Ad-hoc assessments occur as needed and are often conducted by third parties or a subset of current employees who are asked to serve on the ad-hoc red team part-time.

- Applied Critical Thinking (ACT): Decision Support
- Systemic
    - Intelligence Analysis Cycle: As an integrated and regular part of the intelligence lifecycle of a specific unit or type of intelligence
    - Threshold-Based: All decisions that reach a specific threshold (e.g., Acquiring a company, investments of a certain size, targeted assassinations, military action that may prompt retaliation, etc.)
- Ad-Hoc
    - A major event leads a decision-maker to request a red team assessment
    - An existential decision for a company or government leads decision-makers to consider every angle and perspective prior to deciding their next step

Physical Security Red Teaming Overview

Deemed pioneering in the public sector, only a select few organizations employ internal physical security red teams. These organizations protect some of the world's most valuable assets and would face

irreparable damage if they faced a major breach. Technology companies such as Google, Meta (Facebook), and TikTok have posted jobs indicating they have full internal red teams, while financial institutions including UBS, Bank of America, Capital One, and other large banks that hold a significant portion of the world's financial assets, have red teams to test their security systems. As adversaries run into more pervasive digital security measures, they are looking to physical attacks to gain information or access to internal networks. These are often called physical-enabled cyberattacks.

The global Physical Security market exceeded $127 billion in 2022, with an expected increase up to $215 billion by 2030. How do we know that these billions are keeping businesses and populations safer? There are two options that give you real data about whether these security measures work: a red team or a real-world adversary tests them. Waiting for a real incident to occur can have costly and sometimes catastrophic consequences. On the other hand, a red team assessment simulates real-world incidents without introducing the same risk to people, assets, and businesses that a true adversary's attack would. In an environment where adversaries only have to be right once, and businesses need to successfully defend themselves 100% of the time, physical security red teams identify the cracks in the defenses and proactively help fix them before an adversary tries the same approach.

Who Benefits from Physical Security Red Teaming?

Technology companies, banks, government agencies, energy companies, consultancies, and many organizations that protect critical assets, work in high-risk environments, or simply want to have industry leading security, all conduct Physical Security (colloquially referred to as PhySec [pronounced: fizz-sec]) red teaming. When you have significant threats (e.g., North Korea regularly tries to steal your crypto-funds) or assets (e.g., $1 billion of intellectual property, research, or funds) which you want to make sure are safe and secure - a red team is the best tool. Most of the things we value in society are protected by multiple types and layers of security. We have a great deal of faith in these layers of security, relying on them to feel safe and go about our daily business. The best way to determine whether these layers are working is to test them, and to do it before our adversaries do. This is as true for businesses as it is national infrastructure. It is better, safer, cheaper, and smarter to internally test security before someone malicious does.

Why conduct Red Teaming?

Red Teaming is for any organization with high-value assets, serious threats to their business, or which discovered significant vulnerabilities the hard way. Red teaming should enable the business to carry out its mission with greater confidence, less surprises, and no interruptions. A good red team assessment will provide the business with key information relating to:

- **Threat Actors and their Tactics:** The intelligence-gathering and analysis conducted as part of red team operations will define specific threat actors (bad person/group with an objective), document history of their attacks, and identify most likely tactics they are likely to use against a specific organization. This makes it much easier to focus resources and defend against those tactics.
- **Undiscovered Vulnerabilities:** Identify site-specific or global undiscovered vulnerabilities of varying severity. Red teams will often say "better us than them", meaning it is better that an internal team uncover an organization's weaknesses than someone with bad intentions.
- **Addressing Hubris:** As security and risk management professionals, we think we know how to best protect our business, people, assets, and reputation. With stakes this high, even the most

revered experts must be willing to test their decision-making and organization against real-world situations to see if its security measures hold up.

- **Better Budgeting:** Red teams challenge security assumptions and determine whether the money spent on security, compliance, and risk management are truly keeping businesses safer. There are many ways to allocate a budget that will theoretically result in risk reduction. A red team determines whether these measures truly reduce risk, giving organizations confidence and providing the data to be most efficient with resource distribution and security investments.
- **Protecting Assets:** Other than being targeted by real-world adversaries, there is no better way to understand how well businesses are protecting assets than a red team assessment of most valued company assets. Efficient red teams target the company's assets, whether they are employees, knowledge, intellectual property, servers, crypto assets, passwords, company bank accounts, financial assets, equipment, or much more.
- **Protecting Business:** An assumption built on an assumption which is built on another assumption is a house of cards ready to collapse when one foundational assumption turns out to be false. Red teams are assumption assassins. They systematically identify corporate, security, and risk management assumptions and test their validity, equipping the leadership with the clarity and information needed to make better informed decisions. All of this enables the business to operate uninterrupted, minimizing surprises, and strengthening both resilience and confidence.
- **Leveraging Perspective:** Red teamers are experts in security and have a keen understanding of the mechanisms that both drive security efforts and that can stop good initiatives in their tracks. They have been on the receiving end of security measures that make it impossible to breach an organization and have easily evaded expensive security measures that serve no purpose but to create excitement or enrich a vendor. Typically, once on the inside, it is impossible to view an organization through the eyes of an adversary, because most threat actors are unlikely to share where they plan to attack, or which weaknesses they are actively exploiting. A red team provides that external perspective and tests against it, with the added benefit of having seen similar situations and various ways to prevent them from succeeding.

Red teaming is not just a tool; it is a philosophy that challenges the status quo and actively seeks out ways to improve security. It is about harnessing the power of critical thinking to protect the most valuable assets and keep organizations and people safe. By emulating potential threats and assessing a company's defenses, it helps ensure that businesses can withstand the very real and growing threats that exist today. From the Pentagon to tech start-ups, red teaming helps security decision-makers take the guesswork out of security and replaces it with evidence-driven decisions, ensuring that precious resources are directed where they can make the most significant impact to protect the things that matter.

Force Multipliers: Red Teaming & Security Risk Management

If an organization is unwilling to make improvements following a red team assessment, then the red team should not exist. Most organizations face an endless backlog of improvements, upgrades, training, ideas, new technologies, and projects to increase security - all with limited budgets and resources to make those changes. A security risk management (SRM) team is the best tool to identify the most significant risks and most efficient ways to mitigate those risks. A red team provides the SRM team with the data and evidence they need to drive informed decisions and efficient use of security budgets.

The function of security is to serve the organization by protecting its ability to operate (for government) or profit (for businesses). In this role, security teams should find ways to support and enable the business, even if the business disagrees or overrules the security team's decision. A risk ownership and acceptance process can enable business leaders to own and accept a risk on behalf of the business, signaling that they are acting outside of the recommendations of the security team and accepting this risk on behalf of the business for good reasons. This effectively communicates the security team's opinion and recommendation on the risk, allows the business to move forward, and provides top cover to the security team, if an incident were to occur. This process has the added benefit of frequently changing business leaders' minds when they realize the types of risks managed by security teams, and the responsibility that comes with owning those risks. Only rarely do business leaders decide to move forward with the risk acceptance process when presented with the security team's risk assessment, recommendation, and willingness to transfer the ownership of that risk over to another team.

Red teams are only effective when combined with sincere cross-functional efforts to fix vulnerabilities in the security posture of an organization. A red team should be regarded as the most valuable loss-avoidance tool that a security organization has, helping to increase and decrease expenditures based on data collected from operations.

Success stories of unauthorized access, penetration tests, social engineering, acquisition of proprietary information, and making away like bandits with the company's most protected assets are cool stories to tell over a beer; however, the best red teamers truly care about driving positive change in workplace, improving security awareness in the entire workforce, and protecting things that matter to the organization. It is elating as a red teamer to meet the CISO in their chair first thing in the morning after breaking into their office, to send a midnight selfie from a critical server room, or to show that you have access to a billionaire executive on their morning jog with no security. Yet the thrill of a reached objective wears off very quickly if no changes are made, and you continue to defeat the same security system in the same ways again and again.

—

A Case Study in $32M Assumption

A large entity with a high-security facility dedicates $32 million to create strong perimeter fencing and implement bollards. These measures are to prevent unauthorized vehicles from crashing through and running over staff or exploding near or under the facility. The objective of the project is to create a perimeter impenetrable to unauthorized vehicles while maintaining easy access to vehicles permitted inside the perimeter. After the project is complete, the organization hires security officers for each vehicle entrance and pays them minimum wage to determine which vehicles may enter the campus. The agency tasked with protecting the high-profile individuals inside the building believes, rather assumes, that a secure perimeter now exists due to the successful completion of a $32 million project.

During a routine annual review with the red team about key assets, assumptions, and threats to the organization, multiple teams identify that this expensive project created a lot of confidence in the entity's ability to keep dangerous vehicles away from the facility and high-profile leaders. The red team identified that the leaders in the security guard force, the technology team who controls when the bollards retract, and the team that designed and managed the placement of the bollards were not working together, and each made assumptions about how the others were operating. In essence, the security officers viewed

their role as allowing approved vehicles to enter, the technology team ensured that the bollards could retract when authorized, and the physical security design team placed the bollards in a way to prevent unauthorized entities from gaining access onto the grounds.

After hearing all three teams mention how they assumed that their counterparts were operating, the red team prioritized a test of this $32 million perimeter protection system. After surveilling the vehicle entrance for three hours, the team obtained a truck the same size used in the World Trade Center bombing, placed large suspicious (but not alarming) objects in the back of the truck, and drove it directly past the security officers and into the parking lot, placing it next to the sign stating “Reserved for the CEO”. The van was left for six days, with the CEO coming and going multiple times during that period. After nearly a week, the team returned the van to the rental center and began the task of relaying the results to each involved team.

Takeaways:

- Too many assumptions can create a house of cards. In security, the collapse of cards can be catastrophic. Red teams should pay close attention when they hear other teams make assumptions about systems and the roles other teams play in securing particular components.
- Analytical red teaming is a contrarian approach to strategic and operational decision-making that uses a systemic critical thinking approach to make the best possible decision, accounting for unknown unknowns, cognitive biases, assumptions, and other factors influencing objective and sound decision-making.
- Beyond hands-on testing of measures, through the designated role of Devil’s Advocate, red teams should challenge assumptions. A confirmed assumption creates confidence, while a refuted one empowers teams with the truth about the situation, allowing decision-makers to decide whether to act on the findings or accept the risk.
- A red team leader should be a big-picture person and systems-thinker, who understands the security program and the various interdependencies and silos that exist. Often red teams are the only teams thinking about the organization while others work in silos to improve their individual programs or create exclusive silo-suburbs working with a small group of other silos away from the wider organization.
- An effective red team is a silo firefighter, identifying when and where the structure and personalities of the business hamper security progress.
- Red teams are frequently testing security measures and processes that no one in the organization is thinking about.
- Red Team Principles
- Physical security red teams should follow key principles to ensure success and promote a positive culture:
- Independence: A red team should function as a semi-autonomous body within a wider company. Reporting to leaders within security or finance divisions helps establish a good climate for the red team to operate within.

- Their Business is Our Business: The red team exists to protect the organization, company, or entity in which it works. This means the business's goals are the red team's goals, and anything standing in the way of those goals is an adversary that should be examined by the red team. Each red team must therefore understand the business, how it operates, how it profits, and what the key security decisions are.

- Failure Is Success: Operational failure for red teams equals organizational success; red teams serve to illustrate both strengths and gaps in security systems. When a red team is deterred, prevented, or detected during an operation, they should celebrate and set an example of positive reinforcement, which will quickly and positively improve the culture of security and the processes that support it, be it people, process, or technology.

- Loss Avoidance: Since red teams will rarely generate profit for the company or entity, their overall value to the organization should be measured in loss avoidance, or the amount of harm that did not occur because the team identified and helped fix issues proactively. This is often measured by quantifying loss magnitude, and may be estimated using the Factor Analysis of Information Risk (FAIR) methodology.

- Identify Gaps: The red team's goal is to identify gaps in the security measures and provide adequate documentation to inform, inspire, and ensure adequate fixes are put in place.

- Zoom Out: Security departments must always choose the scale at which to address each finding. Do they fix a specific issue, conduct a root cause analysis to determine how the issue came to exist, or conduct an audit of all similar issues globally after a finding? A good red team should understand the scale at which mitigation measures should be recommended.

- Risk-Based Approach: Not every finding needs to be addressed. An obscure and time-consuming method to pick a lock or hack a badge reader should be noted; however, there are a significant range of red team findings that need-not be remediated due to the relatively low likelihood of ever facing those tactics from real adversaries.

- Blameless: Red team assessments offer safe opportunities to fail and should never be a "gotcha" moment or embarrass security teams. It is the one opportunity security leaders have to perform insufficiently as adversaries breach security measures. These are opportunities to practice and learn, and no personnel should be punished, let alone fired, for their performance during a red team assessment. During debriefs, presentations, and follow up conversations, all parties should set egos aside and talk pragmatically about security.

- Reports to Owners Only: Except in rare circumstances, vulnerabilities owners and those with a need-to-know should be the only ones receiving red team readouts. This means the red team is not contributing to workplace politics, and security managers are not surprised with red team results by their bosses or their internal competitors. Those stakeholders who do receive the report from the red team are welcome and often encouraged to share it with a wider audience; however, solely at their own discretion.

- Improve Security Awareness: Red teams can also gamify security for the employee population and security teams alike. Red teams are highly effective and frequently underutilized allies to security awareness teams. Increased awareness from security officers means tailgating, social engineering

attempts, and suspicious items are more often recognized and reported. Security is more aware since they expect to be routinely tested. For the wider employee population, red teams have the opportunity to recognize and reward vigilant employees for catching a red teamer.

Setting Up a Corporate Red Team

Establishing an internal red team to test a physical security organization will be transformative to any open, innovative, and proactive security department. It can be accomplished with nine fundamental steps:

1. Understand the Business
    a. Learn about the business, how it operates, how it profits, and what the biggest risks are.
2. Define the Scope
    a. Determine the scope of the red team.
    b. Identify whether boundaries are drawn at the edges of the physical security organization, or if the team can also test the interdependencies with the physical security organization.
3. Define the Goals
    a. Define the physical security organization's goals. Determine what they are aiming to accomplish.
    b. Develop the red team's goals. Examine how the red team can help the organization and the business achieve their objectives.
4. Define the Mission
    a. Define the red team's level of independence, scope, and engagement with partners.
    b. Determine which Security Objectives the team seeks to test: Deterrence, Detection, Prevention, Response, Delay, Recovery, etc.
5. Establish Red Team Identity
    a. Define suite of services and approach:
        i. Outside in: Operators know little about the security measures and try to match the level of knowledge to that of an adversary. These teams are often removed from the security organization and sit within audit or finance.
        ii. Insider: Close partners to their security peers, these teams will still conduct tests as though they were unknowledgeable outsiders, but they spend most of their time partnering with other security teams on remediation of vulnerabilities and testing of new security features.
        iii. XFN: A team that predominantly partners with cross-functional (XFN) security teams to conduct tests and achieve goals.
        iv. Assurance: A team focused on testing individual or groups of controls to determine whether they are effective, rather than emulating an adversary and carrying out a detailed and relatively unrestrained assessment.
        v. Targeted Assessments: A team that focuses on testing security surrounding specific high-value assets.
        vi. Independent Full Scale: A true red team that has the independence to prioritize, develop, and execute red team assessments based on risks and requirements of the business.

b. Define red team staffing based on need, budget, required expertise: internal staff, vendors, consultants, ad–hoc recruited SMEs.

6. Develop Transparent Communication Channels
   a. Transparency enables red teams to communicate effectively and demystify the mission, where appropriate. It creates an opportunity for leadership buy-in and gives the partners being tested an opportunity to bring to the forefront any security measures of concern, whether that is an incomplete SOP or a misconfigured piece of technology. It is imperative that the communication style used by the red team be clear, frequent, and diplomatic. Early on, each red team leader should:
      i. Create stakeholder maps and establish partnerships. The red team will always require allies in order to be successful (not in the assessments themselves but in the implementation of any resulting improvements).
      ii. Create tiers of communication paths internally, with leadership, with affected (tested) partners, with external partners who will feel the secondary, tertiary, etc. effects of the assessment findings.
      iii. The initial communications should precede the assessments to maximize the breadth of testing for relevant components. The expectation-setting should continue throughout the operational planning, at which time constraints, restraints, and mission objectives will be refined. Legal (do not kidnap the CEO's kids), compliance (do not replicate "borrowed" user data/PII information), operational (do not imitate active shooter), and organizational (we do not want this particular IP prototype to leave the office perimeter) safeguards and scope are established and documented and, where applicable, communicated outside the operational team to external partners and leadership. For the authenticity of the findings, the integrity of the operation, and the de-risking of the red team's mission, red teams hold themselves to the highest level of confidentiality and share the operational information only on strict need-to-know basis.
   b. Create a red team communications one-pager to outline when and how the red team communicates with partners. Focus on transparency and the fact that leadership is read-in to most operations, and leadership decides what additional parties are read in.
      i. Red teams should aim to be as transparent as possible while protecting the integrity of the operations. Information should not be hoarded or used as currency. Radical transparency will quickly allay fears and create strong partnerships.

7. Create or Leverage Infrastructure to Support Red Team Mission
   a. Security Risk Management teams are often the best partner to receive, prioritize, and manage red team findings.

8. Begin Prioritization
   a. Determine inputs needed to prioritize red team operations. These may include Risk and Threat Assessments, Internal Intelligence, Incident Data, External Intelligence, Requests, Leadership Interviews, Team Interests, and more.

9. Ensure that red team leadership is empowered with independence and is granted resources required to train the team to these objectives and carry out the requisite assessments.

Red Team Range

A red team that simply breaks into buildings is like a Swiss army knife being used only as a bottle opener. It fits the role, but it is a waste of resources when you have a tool available that can be used for many other useful purposes. Red teams, like audit teams, should be independent entities that have leadership buy-in and test all aspects of security surrounding the company. A red team in a corporate security setting should be testing:

- Executive Protection Programs
- Event Security
- Crisis Management Teams & Plans
- Investigations
- CCTV Systems
- Access Control Systems
- Security Officers
- Security Awareness of Employee Populace
- Mail Screening
- Third Party Risk
- OSINT Exposure
- SOC/GSOC
- Supply Chain Security
- More: If something plays an important role in the entity's defenses, the red team should test it against realistic and impactful tactics.

Limiting the scope of a physical security red team, whether at the team manager level or the corporate leadership level, can have significant detrimental effects to the security of the company. While the methods of breaking into buildings or computer systems is reasonably well-known in the red teaming industry, tests of executive protection programs, investigation teams, and supply chain security all require creativity and imagination. Unsurprisingly, these creative and unique tests often yield the most interesting and impactful results. Red teams should always seek breadth in their prioritization of assessments and consider teams that have never been tested while simultaneously protecting critically important assets.

Partnering with Other Red Teams

At their peak, large companies can have five or more red teams in place helping to improve their security, services, and decisions. These teams may include privacy red teams, AI red teams, threat modeling teams, hardware red teams, cybersecurity red teams, physical security red teams, product red teams, and more. Red Teams at the same entity can benefit from working together. Framed differently: An adversary will not have the same silos that security organizations, including red teams, do. Many adversaries are well-funded groups with substantial resources and training, who may cross boundaries from a cyberattack to physical attack, to the theft of data, to the manipulation of an algorithm or abuse of a product without hesitation. The adversaries have the advantage of pursuing their objectives without boundaries or silos. To counteract this dynamic, red teams should collaborate across those same boundaries to emulate and counter them.

Working with entirely different and often unrelated teams may be difficult, however. A first step to begin cross functional partnership may be as simple as brainstorming ways of how an adversary may attack. Poison Circles are used for both threat ideation and scenario development at different points in the red

team process. They are structured brainstorming exercises to discuss possible attack plans or relevant techniques a threat actor may employ. These exercises are intended to both bring imagination and plausibility to the assessment process while challenging stereotypes, preconceived notions, and groupthink. Much like adversaries may draw their inspiration for attacks from a variety of sources, systemic brainstorming through Poison Circles allows the red team and other security experts to do the same. As red teams collaborate with each other, or a primary multi-functional red team grows to include additional dimensions, there are several models that have shown efficacy in producing effective operations.

Ways to Work Together Working with Related Red Teams

Red teams can work together in many ways, from occasional conversations to fully integrating with each other on projects. All red teams have the same overarching objective: to strengthen and improve the business, government, or entity in which they operate. Regardless of their specific focus, teams may follow one or more of the tested collaborative models, used by the authors regularly to test and improve important systems:

- **Embedded Red Teamer:** A cybersecurity red teamer joins the physical security red team for an operation, or vice versa. The key is to fully integrate a member of another red team through the entirety of an operation.
- **Attend Debriefings:** The debriefing and report following a red team assessment are the most essential steps to ensuring the team's findings are understood, taken seriously, and addressed. Seeing how other red teams present their findings is essential to improving your own approach.
- **Joint Training:** Inviting another red team to attend a training that your red team is hosting, or collaborating on a training that applies to both teams, creating bonds and shared knowledge between teams.
- **Conferences:** Whether just attending, or putting on a joint presentation, the opportunity to bond, collaborate, and share ideas in an exciting setting like a conference will provide huge benefits to the teams.
- **Prioritization:** Effective red teams prioritize based on real-world threats to the company. Each team should therefore have related priorities, presenting an excellent chance to collaborate on joint operations for the year. These sessions present an opportunity to plan to test the same set of security measures from different angles, the target locations via different or combined means, and to ensure all important operations have the proper staffing and resources to be successfully completed for each of the teams.
- **Happy Hours:** This one is simple! Someone needs to plan and host a happy hour for red teams. Attendees have a major part of their professional and often personal life in common with each other at a red team happy hour, creating a great foundation for ice breaking, conversations, and, at times, even future operational ideation.
- **Shared Interest Events:** Many red teamers love lockpicking, no matter what type of red teaming they pursue professionally. Others may have an affinity for threat ideation or desire to debate the best techniques from the Army's Red Teaming Handbook (yes, I'm serious, I know plenty of these folks and they are awesome). No matter what the shared interest, there is always an opportunity to host events and invite the broader community.

- **Recruiting:** Red teaming is exciting. Sending members from several red teams to a recruiting event is a sure-fire way to get the attention of smart and creative candidates who are interested in having fun while contributing to the safety, security, and better decisions of a company.
- **Group Chats:** This one seems obvious, but it takes effort. To establish the foundation of collaboration and likeness between teams it is highly beneficial to have a shared forum for sharing thoughts and articles. There are highly relevant and interesting articles in the news on a regular basis. Having several active participants sending and discussing recent industry news (e.g., heists for physical security teams, breaches or exploits for cybersecurity red teams, etc.) will foster connection between the teams.

There are many more ways that various red teams can work together despite their different focuses and skillsets. It's incumbent upon those teams' leaders, formal or informal, to foster those connections and create opportunities to learn from sister red teams.

The Future of Physical Security Red Teaming

There is sparse public literature about physical security red teams, with the majority or information available in a smattering of YouTube Videos, conference presentations, and notes on LinkedIn. The physical security red teaming profession would benefit significantly from an advocate such as CART, frameworks such as MITRE's ATT&CK or TIBER-EU, information sharing mechanisms, defined KPIs, maturity models, academic studies, expert training, and certifications for individuals and teams, and more. Cybersecurity red teams from industry and government have regular conferences to learn from one another, discuss challenges, and move the profession forward. The same teams have online communities to share news, discuss industry changes, and exchange key findings on a daily basis.

The physical security red teaming lacks each of these key professional milestones, despite a growing industry and increasing number of major global corporations and government entities posting physical security red teaming job positions. As physical security red teaming further takes a wider foothold, several key milestones must be met to mature the profession.

1) **Education**
   a) Formal Education Programs: Develop university courses or centers of excellence that offer degrees, certifications, or courses specifically tailored to red teaming.
   b) Training and Workshops: Organize regular training programs, workshops, and seminars to enhance the skills and knowledge of professionals.
   c) Internships and Apprenticeships: Establish platforms where novices can learn under the guidance of experienced professionals.
2) **Research and Development**
   a) Research Institutions: Create research institutions or centers that focus on developing new techniques and tools for the profession.
   b) Establish Reputable Journals: Develop journals and publications that allow for peer-reviewed professional information sharing within the field.
   c) Academic Publications: Encourage the publication of peer-reviewed articles in reputed journals to enhance the body of knowledge.

d) Conferences and Symposia: Host regular conferences where professionals can share knowledge, network, and collaborate on new projects.

3) Standards and Regulation

a) Certifications: Develop certifications that set a benchmark for the skill and knowledge levels required in the profession.

b) Maturity Framework: Design a framework that helps organizations assess the maturity of their physical security red teaming efforts.

c) Regulatory Bodies: Establish regulatory bodies to oversee the profession and ensure that standards are maintained.

4) Information-Sharing

a) Professional Associations: Establish professional groups to network with other red teamers and establish information sharing frameworks.

b) Resources: Create tools, knowledge, and collaborative platforms to better collaborate and drive the industry towards maturity collaboratively.

Many physical security red team professionals speak at conferences, create videos, appear on podcasts, publish resources (GitHub, LinkedIn, Substack, etc.). Yet with these red teamers moving broadly in the same direction by publishing information, there are still not professional entities, frameworks, dedicated groups, journal articles, or academic courses dedicated to physical security red teaming. There exists a tremendous amount of momentum, interest, and passion about the field of physical security red teaming. The field appears primed to be a standalone profession, on the precipice of maturity and growth seen by many related professions as global profits, governments, and infrastructure become reliant on effective security and defenses that need to be tested and improved regularly.

Story Outro

No prototypes were harmed in the outcomes of this red team assessment. In fact, the prototypes stolen by Ana were returned unharmed later that day and were immediately safer as a result. A multi-functional team made up of leaders and experts from physical security, cybersecurity, R&D teams, lab owners, finance, and facilities management all teamed up to develop plans to quickly patch significant vulnerabilities at the site, while another team focused on global, systemic, long-term fixes to the culture, standards, awareness, and strategy of security across the entire company. A single red team assessment can be the inspiration and spark that leads to significant positive security change, making it a highly efficient and effective step to reduce risk, protect assets, and ensure businesses can operate with confidence.

As for the buildings, labs, and researchers involved in the red team theft of the prototype medical device, there were significant changes made in the days, months, and years following the assessment. New funding for improving the security of these devices was unlocked by the finance, R&D, facilities, and security teams. Local security managers, backed up by top-notch regional security leadership, took the bold move of circulating the red team findings to lab owners, researchers, and employees. This led to the most impactful, sustained positive changes in security posture. Intellectual property protection was a key consideration, with R&D leaders becoming the loudest advocates for practicing good security hygiene. Creative solutions were developed in partnership with researchers to create new solutions that are both convenient and secure, a rarity in the security world.

A few key takeaways include:

- Red Teams exist to test and improve important systems.
- Red Teaming can generally be split between Critical Systems Testing (CST) and Applied Critical Thinking (ACT).
- Companies and Governments will often have multiple red teams.
- There are more types of red teams than just physical security and cybersecurity teams.
- Red teams should work together regularly. The extent and ways that they work together should be determined by the teams.
- There is generally a lack of literature on the various types of red teams that exist in government and the private sector.
- There is ample opportunity, resources, and passion to grow and mature the physical security red teaming profession.

Note: The story in this article is an amalgamation of multiple red team assessments across multiple states conducted in the past decade and a half of red teaming. Each of the vulnerabilities has been addressed by clients and are no longer able to be exploited as referenced.

Authors: Shawn Abelson is a physical red teamer, security researcher, and the Director of Operations at Pine Risk Management. Shawn built the physical red team at Meta (Facebook), and helps companies and governments conduct security assessments safely and effectively.

Ana Aslanishvili is the CEO of a consulting firm that provides security consulting, red team assessments, and risk management support. She has experience in finance and technology sectors conducting investigations, safely overseeing physical red team assessments across the globe.

Professional Analysis

Transitioning from Government to Private Sector Intelligence

Scott Stewart

Although I made the transition from the government to the private sector over 25 years ago, over those years I've had the opportunity to train, lead, work with, and mentor, scores of analysts who were themselves making the transition. Here are several things I've learned over the years and have shared with others. While I'm writing this for the International Protective Security Board Journal and will focus on protective intelligence analysts, the principles I'm sharing are relevant to any analyst making the jump.

Congratulations you're now a generalist!

Government agencies have the resources to hire large teams of analysts and as a result, many analysts are able to specialize, and sometimes in very esoteric areas. In some cases, analysts spend their entire career studying one topic very deeply. For example, I know analysts who exclusively studied Warsaw Pact hand grenades, biker groups in Texas, the flow of methamphetamine precursor chemicals, and Iraqi Shia militant networks in Iraq.

Private sector intelligence teams are usually understaffed and by necessity must be lean and mean. This is doubly true for protective intelligence teams, which tend to be even smaller than competitive intelligence, market analysis, and other corporate analysis shops.

As a protective intelligence analyst, then, you must develop a solid understanding of the entire array of actors who could pose potential threats to your company and principals as well as the various tools and tactics they may employ. This list can include terrorists, criminals, activist groups, aggrieved customers, foreign intelligence agencies, paparazzi, and mentally unbalanced individuals with a focus of interest in your principal or company, among others.

Becoming a generalist requires a bit of mental flexibility but is not a difficult transition for a well-trained analyst. While deep expertise is certainly valuable, if an analyst possesses a well-developed set of analytical skills, they will be able to collect information and conduct a meaningful assessment on almost any topic -- and trust me, you will receive assignments to assess some very odd topics.

Look at the big picture

Closely aligned with the specialist/generalist discussion is the need to look at the big picture. Many analysts who come out of the military or law enforcement spend a lot of time focused on their topics at a very granular level. For example, they may be attempting to help take down a specific street gang or militant cell. This is very important work, but many times they are so far down in the weeds analytically that they do not see the bigger dynamics that are shaping the behavior of the things they are intently studying. For example, I have talked to law enforcement analysts who were laser focused on a Mexican cartel sub-group operating in their city, but they don't understand how that group fits into the larger cartel, or the dynamics between the various Mexican cartels.

Certainly, as a protective intelligence analyst there are times when you will have to dig deep into a subject if you are working up a background on a person of interest (POI) or even a formal threat assessment. There are also instances where you will have to intently focus to identify a social media poster who made a threat.

However, a good protective intelligence analyst must also take the time to zoom out and examine the trends and dynamics that are driving the behavior of threat actors at the macro level. For example, the security company TorchStone publishes a monthly report on threats to high profile individuals precisely in order to keep tabs on broader trends and dynamics that re relevant to Executive Protection teams that need to stay focused on their immediate surroundings, too.

A recent example of these higher-level dynamics would be the way climate extremists have begun to "personalize the cause" by denouncing and targeting specific executives instead of just targeting their companies or organizations. They are also expanding their focus beyond energy companies to financial institutions and individual investors who invest in energy companies, and even companies that support the operations of energy companies. Such a shift in focus by these extremists will have significant implications for many protective intelligence teams.

Flexibility is not optional

Flexibility doesn't just apply to the ability to analyze new topics or to focus on higher level dynamics. Analysts must also be willing to adapt to new ways of presenting their assessments and to using new tools.

In terms of presenting analytical findings, I know it may break the hearts of "PowerPoint Rangers" to hear this, but very, very few people in the private sector are willing to sit through a 58 slide PowerPoint presentation outlining your assessment.

Intelligence is produced for the decision maker, and analysts must adapt to how their decision maker best digests information. Protective intelligence providers are constantly adjusting how we present information to our various clients based on their preferences and corporate cultures. It is far easier for analysts who work for a single company and only have one corporate culture and one decision maker to serve.

Concerning presentation, analysts breaking into the private sector must often learn to write for private sector readers. This means dropping most acronyms and abandoning esoteric military or law enforcement terminology. Some analysts feel the need to impress their new civilian bosses or to prove their bona fides or mastery of a topic by using buzzwords, but this often backfires. Presenting a well-reasoned assessment in clear English will do far more to impress them.

Speaking of clear English, very little will damage an analyst's credibility faster than typos, simple factual mistakes, and grammatical errors. It is a good policy to have at least two sets of eyes on any product that is going to a consumer, and hopefully that second set of eyes is a good proofreader. If an analyst struggles with writing, they should experiment with tools like Grammerly, consider taking some writing courses, or even hiring a part time copy editor.

The mention of Grammerly is a good reminder of all the powerful new tools that are now available to analysts, to include some that utilize some degree of artificial intelligence (AI).

When I first left the government, I missed the flow of information I had access to, not just in terms of classified material, but also all the foreign press reporting that came in via the Foreign Broadcast Information Service (FBIS) and BBC Monitoring. However, it did not take long for the Internet to replace that flow for me and today I really don't miss not having access to classified information flows.

Today almost everyone on the planet is carrying a smartphone that can record photographs, video, and audio – and then immediately upload it to the internet via a cell phone tower. I am astounded by the amount of information that is available about an incident almost immediately after it happens.

This huge increase in information is incredibly valuable, but it can also be overwhelming. However, the challenge can be met by using the proper tools, and even older analysts can be flexible enough to learn to use new tools. Over the past three years, I've learned to use systems like Samdesk, Ontic, and Liferaft Navigator to help me process the rivers of information flowing at my brain on a daily basis. These systems help me from becoming oversaturated with data, something I refer to it as "electronic waterboarding."

While it can at times be challenging to wade through rivers of data—especially when those rivers contain potentially fatal undercurrents caused by misinformation and intentional disinformation—it is often quite possible to conduct a detailed protective intelligence assessment of events that take place across diverse parts of the globe based solely on information obtained from the Internet.

Focus on prevention

In the law enforcement world, officers and analysts must wait for a crime to be committed before they can act. For example, the FBI cannot open an investigation without a criminal predicate. Because of this, the focus in the law enforcement world is on solving crimes and bringing perpetrators to justice. The statistics by which law enforcement officers and agents are gauged are based on arrests and prosecutions.

In the protective intelligence world, however, the focus is squarely on prevention rather than prosecution. Avoiding an incident is always far better than responding to one. Because of this, the focus of protective intelligence analysts must be different from that of law enforcement analysts. I refer to this as focusing on the "how" rather than just the "who."

While in some cases protective intelligence teams do have a "who" to focus on because an individual has expressed a grievance against, or otherwise demonstrated a concerning focus of interest in a principal, potential assailants don't always self-identify to security teams before they begin their journey down the pathway to violence.

Because of this, protective intelligence teams need to rely on analytical frameworks such as the attack cycle, that can help them to recognize and contextualize pre-attack behaviors. Many of these behaviors do not cross the line into criminality. For example, an individual standing on a sidewalk watching a motorcade depart from a corporate headquarters has broken no laws. Conducting Internet searches seeking to determine the home address of a celebrity or corporate leader is not illegal. However, when protective intelligence teams focus on detecting these elements of the attack cycle such as preoperational surveillance – the "how" of an attack – it can then lead them to a "who" they can begin to focus on identifying and assessing. Identifying attack cycle behaviors early can also help security teams adopt additional measures to mitigate or avoid potential threats, even when no law has been violated.

Network, network, network

While networking is extremely helpful for government analysts, it is critical for private sector analysts who have far more limited resources than their government counterparts. There are a number of formal networks such as the Association of Threat Assessment Professionals, the Analyst Round Tables, and OSAC country, thematic, and regional councils. Live events such as the IPSB conference, the OSAC annual threat

briefing, and the Ontic Protective Intelligence Summit also provide excellent opportunities to meet and network with analysts who have shared interests and concerns.

During normal times, my team and I are nearly always in daily contact with someone either seeking information from us, or who we are reaching out to for help. But as I write this, we are a week into the Israel/Gaza war, and in the midst of such a crisis event, my team and I are in hourly contact with others, if not multiple times an hour. In such a situation, it is invaluable to have contact with people who can deliver ground truth an analyst can use to advise their decision maker.

Make a call

Lastly, I want to encourage analysts to have the courage to make a call and provide their best assessment of a given situation rather than prevaricating. Decision makers know analysts are not prescient. They also know and expect that analysts will occasionally make wrong assessments. However, if a decision maker asks an analyst for their best assessment of a situation so that they can make a decision, the analyst must not hesitate to provide the best assessment they can, given the facts available to them. Of course, assessments can and should be adjusted as new information becomes available.

When an analyst makes an incorrect assessment, they must then do an honest after-action review to determine why their assessment was incorrect. Sometimes, assessments are incorrect because of incomplete information, or because a threat actor behaves in an unpredictable manner, but other times they are the result of a logical or analytical fallacy, and in this case, the fallacy must be identified and corrected to prevent a repeat.

I've also learned over the years that decision makers are forgiving when an analyst is transparent about their mistake and explains why it was made – and what is being done to remedy the cause. Owning up to a mistake is far better than attempting to make excuses for or ignore an incorrect call.

Author: Scott Stewart is the Vice President of Intelligence at TorchStone Global, and he has more than thirty years of experience in both public and private sector intelligence, including with the military, federal government, and security companies.

Seeing, Not Just Looking: The Nature of Close Protection

Scott Hamer

On May 4, 2023, the Prince and Princess of Wales arrived on foot to visit The Dog and Duck Pub in Frith Street, Soho, London, W1. Not long after their arrival outside the venue, a male was seen to wander into the allegedly secure area, and it was quickly branded a "security fail" by many commentators on social media. However, was it really a security fail? Did anybody die? Was anybody assaulted? Was the safety of the principals compromised in any way? The answer to all three of those questions is, of course, no. But one can understand why it looks like way. In order to truly assess the risks, one needs to see, not just look.

Understanding Close Protection

Before engaging in the scenario mentioned above, it is important to start with the question: what is close protection? Close protection is not just about denying all access to a principal (the person being protected). That is what a bodyguard does. Put simply, protection officers are responsible for the last ten feet. Generally, they have to work in concentric rings of security layers provided by somebody or something else. There's a lot of trust in those outer rings and a lot of responsibility for the last. The Personal Protection Officer (PPO) is responsible for what happens in that last ten feet. It is a big responsibility, and a cool head is required to do the job properly.

If we really wanted to protect public figures with no chance of any compromise or attack whatsoever, the reality is they would be closely guarded in secure premises with lots of security features and never have any interactions with anybody unknown or the general public. Unfortunately, that does not fit in with the wishes of most public figures. They are expected to be accessible, and they expect to be accessible. In my experience those who want close protection don't need it, and those who need it don't want it. Whilst it

can be a nice talking point or fashion accessory for those who think they need it, for those who do, it is a massive imposition on theirs and their families' lives.

The protection officer has to assess, then allow or deny, many interactions with his or her charge on a daily basis. It isn't an easy task. It requires intelligence. Not just the obvious ability to comprehend but also emotional and social intelligence is required in abundance too.

Difference Between Body Guard and Close Protection

Well, generally speaking, anyone with muscles and size can be a bodyguard. A physical, sometimes intimidating presence hopefully deters people from approaching or attacking the principal. It is not much more than that and does not require much security training or experience. The bodyguard believes that their mere presence on its own will prevent an attack, and they generally will only ever respond or react to a given and obvious threat.

For example, there is the news footage a few years ago when a public figure was appearing in a high-profile case at a London court. He was surrounded by tough bodyguards who pushed their way through the crowds and the media frenzy to the front doors of the court only to find them locked. The principal then had to stand outside the front doors in an embarrassed silence as the media pack threw questions and aimed their cameras at him while the bodyguards uncomfortably attempted to maintain a ring of bodies around him until the court opened. It is all they could do. There was clearly no Plan B, nor any contingencies considered. Their only objective was to get their principal in through the front door.

On the other hand, the close protection officer will understand and acknowledge their vulnerabilities. They will make plans to reduce the likely risks and have a number of contingency plans to fall back on should something happen. The close protection officer is constantly assessing, watching, seeing (not just looking), and reassessing. You will see them watching the crowd, not the principal. They never need to touch a principal, unless it has all gone wrong. They let their principals go about their business and lead their daily lives, blending into the background, unless there is a real need to intervene.

Close protection officers, assigned to the court task above, would have researched the court, completed a recce, had a Plan B-D, would know what time the doors opened, would have had an advance, would have communications, and would have scoped out alternative methods of getting into the court as an absolute minimum.

Necessary Training for Close Protection

Now, while everyone with an SIA Close Protection badge will call themselves as close protection officers, the reality is most of them have only ever completed an initial bodyguard course. The SIA course is just 194 hours of training (previously having been 150hrs). Many will not do much more training than that.

It is no secret the Royals are protected by police officers from The Metropolitan Police's Royalty and Specialist Protection Department (RaSP) - a department I was part of, in various iterations, for just over half of my 30-year police career. There's a lot of reasons why the police protect public figures. They have lots of experience of dealing with the public, dealing with confrontation, mental health, and much more.

No new protection officers get to look after the UK's most high-profile figures. They have to cut their teeth on the 'minor' principals for a few years first. Prior to this they have undertaken one of the most comprehensive close protection courses anywhere in the world, which includes at least six months of

dedicated training and, once successful, continual refreshers. Prior to that, most have spent at least five to ten years on the streets of London honing their people and conflict management skills. They are very good at "reading" people. Good cops make good protection officers. Managing shades of gray is the skill. Close protection is rarely black or white.

Assessing the Security Fail

So, was it a security fail when a man entered the "secure area" around the royals? Probably not. Knowing the principals, the officers, and the training and protocols, there was no real threat posed by the suspect. One can never say never, of course. There is always some risk, but the difference between a good close protection officer and a mediocre bodyguard is that the protection officer is always assessing the risks. He or she is seeing, not just looking. They have spent as much time studying the art of close protection.

There are several important points in assessing the breach and whether or not it was a "security fail." How did the principals arrive? They took the Underground and walked to the pub. The trains were full of morning commuters, meaning the trains would not have been searched and the two principals would have mingled with lots of unscreened members of the public on the train, the escalators, and the commute. Therefore, does one more member of the public who inadvertently finds himself in the middle of a Royal arrival on an open public pavement really present a real security risk? Probably not.

In that split second a very quick risk assessment needs to be made. Of course, security officers all realise it is better for the operation if the suspect were not there, but a good protection officer will have quickly considered and assessed the situation unfolding. The kind of assessment a close protection officer would make would consider the following questions for each aspect of the situation:

- Person: Is the individual posing a threat? Does he / she have the current capability to commit an assault on the principals? Is the person exhibiting any obvious signs of intention to do our principals harm? Does the person's body language support this premise? In this example, the suspect displays a number of behavioural signs consistent with being in the wrong place. He does not appear to be very aware of his surroundings. He looks a little startled when challenged, realises he is probably in the wrong place, and is quick to show the officer he has just been to collect a prescription.
- Object: Is there an obvious weapon? The man is carrying a bag. It could contain a weapon. What kind of weapon could it be though in a paper bag? A viable IED, a gun, a knife? Observation indicates that it was a paper bag from a pharmacy and extremely unlikely to contain anything of substantial weight.
- Profile and Wishes of the Principal: How would the principal expect their protector to react in this scenario? Will the protector's actions become the main story? Will the protector's actions embarrass the principal? While these aspects should never override safety and security, reputational concerns must always be part of one's risk assessment.
- Environment: Does this person fit into this environment at this time? It's an open, public street scene. The road has not been fully closed. Pedestrians are free to move in the street. Barriers are in place for the press, but the public still have free movement in the street. With some local knowledge, and having completed a good recce, the protectors should know there is a pharmacy in the same street near the pub along the route taken.

As well as the obvious protection officers around the couple, there would have been a number of additional covert and technical assets deployed around the couple to make it look like the couple have just decided to take the tube and have a nice walk. Not to mention the weeks of planning that would have gone into it. The whole point in being a public figure is to get among and meet the public. Close protection officers are enablers.

As an official engagement, the press was in attendance, and some pedestrian barriers were placed to manage them. No barriers were used to stop the public or pavement flow. Generally, the British police do not close down streets for such visits. The principals do not want to inconvenience the public. Normality is allowed to continue, and the protection team manages the risks, the vast majority of which have been pre-considered with a contingency option.

When the personal protection officer identified the errant male, he did his job perfectly. He reacted quickly, had a presence, and unobtrusively managed the situation. All of that is the hard part. Anyone can look, but close protection officers need to see what is happening around them and be able to apply their deep training to quick risk assessments. That is what separates the close protection officer from just a bodyguard.

Author: Scott Hamer was a senior manager in Royalty and Specialist Protection with the Metropolitan Police, and he was a Personal Protection Officer to His Majesty King Charles III. In addition, he has worked as the personal protection officer for a number of other high-profile public figures in the United Kingdom.

Selecting Suitable Programs in the World of Defensive Tactics Training

Alan Baker

In the world of defensive tactics training, technique-based programs have been prevalent for a long time. However, many customers need to be aware that better options are available. This article will explore the significance of incorporating thought tools and body state training into defensive tactics programs to improve practitioner skills and enhance overall effectiveness. By understanding the importance of these elements and making informed choices when selecting training programs, individuals can avoid low-value offerings and invest in training that truly prepares them for real-world scenarios.

The Need for Thought Tools and Body State Training

Thought tools and body state training are not easily mastered, but they can elevate a practitioner's abilities when applied effectively. Unfortunately, many traditional programs do not include these essential components due to instructors' lack of knowledge and training or a preference for more straightforward teaching methods. As customers, it is vital to seek programs encompassing both technique-based training and the development of these mental and physical attributes.

Thought Tool Training

A thought tool represents a principled, holistic approach to learning that goes beyond mere techniques. When observing practitioners who excel in their fields, it becomes evident that their prowess is not just about skill – it is about how they think. These top-tier individuals often differentiate themselves by their unique and elevated perspectives. Their advanced thought processes, characterized by depth and nuance, often set the stage for their outstanding performance.

So, the challenge for educators, mentors, or program designers is clear: How can they instill this refined perspective and elevated thought process in their students? Essentially, "thought tools" describes teaching methodologies that focus on shaping the learner's mindset. An effective learning program should not just offer techniques; it should integrate strategies that prompt students to reconsider their understanding of these techniques. By understanding the power of this approach, individuals can make more informed decisions about their training avenues and select programs that foster a deeper, more intricate understanding of their craft.

Body State Training

One must not overlook the crucial component of body state training when assessing training programs. This aspect transcends mere techniques or cognitive patterns; body state training delves into the physical condition in which a practitioner applies a technique. It is the nexus between the mind and body, where the physical state directly influences the outcome of an applied technique.

To illustrate, consider the concept of tension within the body during high-pressure situations. Elevated levels of flexion or tension act as a roadblock to optimum performance, akin to driving with the handbrake engaged. An excessively tense body hampers your athletic ability, making you less formidable in physical confrontations.

This phenomenon is evident in martial arts academies, especially among Jiu-Jitsu practitioners. Unlike their seasoned counterparts, novice Jiu-Jitsu students often display a discernible tension when exposed to a demanding environment. Experienced practitioners, having honed their art over time, maintain a relaxed demeanor. This relaxation doesn't signify weakness; on the contrary, they appear more substantial, exuding an aura of strength, making them seemingly immovable to their training partners.

By mastering one's body state, particularly the control over tension and flexion, an individual can enhance their athletic performance manifold. The benefits are not limited to improved agility or speed; a relaxed state ensures the maximum number of muscle fibers are at your disposal, ready for explosive contractions and dynamic force when necessary.

The study of tension represents merely a facet of the expansive domain of body state training. Numerous elements await the eager learner, each contributing to holistic development. However, as with the concept of 'thought tools,' a comprehensive training program should incorporate a robust curriculum focused on body state education.

Delving into body state training demands patience and commitment. It's a nuanced field requiring understanding and physical integration, making it a challenging pursuit for many. This intricate nature, coupled with the considerable effort required for instruction, often deters many trainers from incorporating it into their programs. The industry, unfortunately, is saturated with programs that prioritize ease of delivery over comprehensive education.

Yet, true mastery and profound growth lie in embracing these intricate training modules. Students require this deep-seated knowledge for genuine transformation and to foster advanced skill sets. Therefore, as one navigates the vast landscape of training options, prioritize programs emphasizing body-state training. Such programs, while rare, are the bedrock of genuine expertise and the hallmark of elite training institutions.

The Role of a Skillful Program Designer

To create an effective defensive tactics program, a designer must possess a comprehensive background in a full spectrum of combat disciplines. This should include firearms systems, edged weapon systems, blunt weapon systems, striking, hand fighting, pummeling, takedowns, grappling, and ground fighting, among other essential techniques. A well-rounded program gives students a holistic understanding of self-defense, ensuring they are prepared for diverse threats and situations.

In addition to a diverse martial arts background, a proficient program designer must thoroughly understand firearms training. Firearms are an inescapable reality in defensive tactics, making it imperative for the creator to be well-versed in this domain. Similarly, expertise in edged weapons is equally essential. An ideal teacher or program designer should boast proficiency in at least multiple martial art systems accompanied by knowledge of a military blade system. This comprehensive grasp of different weapon systems enables the designer to craft a well-rounded and practical training program that equips participants to defend themselves against a range of threats and challenges effectively. Drawing from a wealth of combative knowledge, the designer elevates the training experience, providing students with invaluable insights and a holistic approach to self-defense.

Beware of "Experience"-Based Events

Some programs prioritize creating an exciting and immersive experience over providing quality training. These "experience"-based events may leave participants feeling satisfied, but they offer little substance and are often built on flawed information and designs. Customers must distinguish between genuine training and gimmicks, ensuring their investment is truly valuable. For example, Sanrio-based training undeniably holds immense value, provided it rests on a foundation of solid training principles. The essence of this approach lies in embracing non-systemized thought, encouraging practitioners to think outside the confines of rigid systems.

Customizing scenarios to fit the participants' unique environments is essential, avoiding a one-size-fits-all approach dictated solely by the opinions of a system. However, it is worth noting that some training programs might misuse Sanrio-based methods as a means to mask their inadequacies and deficiencies. Hence, it becomes crucial to discern authentic and effective Sanrio-based training from superficial attempts designed to compensate for poor program quality.

The Importance of a Diverse Background

One prevalent challenge among defensive tactics program designers lies in their constrained background in martial arts and other related systems. Crafting a truly comprehensive and effective program requires a diverse range of influences to draw upon, which demands considerable time and effort to obtain. Regrettably, many designers fall short in this aspect, resulting in the development of incomplete and ineffective training programs.

An effective defensive tactics program should encompass an array of techniques, strategies, and principles sourced from various combat disciplines. A well-rounded designer must possess knowledge and experience in a plethora of martial arts systems, including but not limited to firearms systems, edged weapon systems, blunt weapon systems, striking, hand fighting, pummeling, takedowns, grappling, ground fighting, and counter-grappling methods. By integrating elements from different disciplines, the designer can create a cohesive and versatile training regimen that addresses a wide range of potential scenarios and real-world encounters.

Moreover, an astute program designer must be open to exploring non-systemized thought and be willing to adapt their training scenarios to the participants' specific environments and circumstances. This flexible approach ensures that the training remains practical and relevant, catering to each individual's unique needs and challenges. Rather than adhering rigidly to the dogma of a single system, the designer should prioritize the development of critical thinking skills and problem-solving abilities within the participants.

Tailoring Training to the Terrain: The Environmental Design Imperative in Martial Arts Programs

When selecting a martial arts or defensive tactics program, one cannot stress enough the importance of environmental compatibility. A significant number of martial arts systems available today do not possess this specialized design. They often offer generic solutions for intricate situations. For protection agents, the day-to-day reality of their profession involves operating within varying force levels. A deeper look reveals that most of their interactions are, in fact, on the lower end of the force spectrum, such as politely handling an overly enthusiastic fan of a high-profile client.

Conversations with industry veterans underscore this point. While full-fledged physical confrontations are rare, low-level threat physical exchanges are frequent. This disparity highlights a gap in the majority of martial arts systems, which are heavily biased towards high-intensity engagements. Recognizing this imbalance is crucial, and programs should pivot toward providing holistic solutions suitable for protection agents.

Thus, the assertion emerges: a top-tier program must be designed with the environment in mind. It should be mindful of daily wear, modes of transportation, predominant environments, legal implications, and client-imposed stipulations. Whether an agent is armed or unarmed, the training should address all these facets right from its inception.

Digging Deeper: Essential Elements of Environmental Design

1. **Public Perception and Optics**: There are omnipresent cameras and social scrutiny. Training should focus on more than just effectiveness and pass the public's eye test. The tactics employed should strike a balance between being socially acceptable and operationally effective.
2. **Strategies Tailored to Locations**: Environments have distinct challenges. Training should offer strategies specifically curated for diverse settings, whether it's a crowded event or a silent hallway.
3. **Understanding Organizational and Legal Boundaries**: Professionals should always be apprised of their operational limits. This covers the broader legal framework and nuances of organizational guidelines.
4. **Justification and Accountability**: Beyond physical tactics, a professional's training must also equip them to explain their actions. This ensures accountability, allowing agents to convey the reasoning behind their decisions when needed logically.

Addressing the Real-world Challenges

Environmental aspects aside, it is also essential to factor in the logistical constraints that professionals face. The notion that traditional martial arts training can effortlessly integrate into a professional's routine is misguided. Time constraints necessitate that the training content be concise yet potent, promoting self-driven progress and continuous evolution. An environment-centric program, enriched with an understanding of professional constraints, stands out in the crowded space of defensive training. It goes beyond mere techniques and ensures the learned tactics resonate with the multifaceted challenges professionals face daily.

Choosing the Right Program

When considering a defensive tactics training program, it is essential to research both the training event and the person behind its design. Look for programs that incorporate thought tools and body-state training alongside technique-based instruction. A designer's background and expertise should encompass multiple combat disciplines to ensure a comprehensive and well-rounded curriculum. Prospective trainees must assess program designers' backgrounds and qualifications before enrolling in defensive tactics training. Seeking a designer with a well-rounded experience and understanding of multiple systems increases the likelihood of receiving high-quality and effective instruction. A comprehensive program

designed by an experienced professional will offer valuable insights, equip participants with practical skills, and foster the confidence needed to handle various real-life situations effectively.

The gravity of defensive tactics training should always be considered, as it serves as a pivotal factor in preparing individuals for life-threatening scenarios. By prioritizing programs that incorporate thought tools and body state training, participants gain a distinct advantage, elevating their capabilities and real-world effectiveness. The selection of a training program should be approached with careful consideration, with a keen focus on the designer's qualifications and background in a wide array of combat systems. Armed with this discernment, individuals can make informed choices, investing in defensive training that yields tangible results, bolstering their personal safety and instilling a profound sense of confidence and assurance. With a commitment to comprehensive and skillful training, individuals are better equipped to protect themselves and others, making their communities safer and more secure. Remember, the path to mastery in defensive tactics is not just about the technique but about the application of knowledge, critical thinking, and an adaptable mindset – all of which can be fostered through a thoughtful and well-rounded training program.

Author: Alan Baker is a martial arts and self-defense expert and leads Baker Defensive Tactics (BDT), teaching countermeasures and cutting-edge defensive tactics, firearms, and edged-weapon programs to corporate security teams and law enforcement departments. In addition, he founded and is the principal trainer for the Civilian Tactical Training Association, C-Tac, to bridge the gap between martial arts and “self-protection.”

Submitting to the Journal

The Close Protection and Security Journal is a bi-annual publication, and we welcome submissions from scholars, researchers, and practitioners on a number of topics. The scope of the Journal is intentionally broad as there are currently no scholarly publications dedicated only to corporate security. Importantly, the intention of the Journal is to be a scholarly publication led by practitioners, offering their in-depth insights into historic cases, current issues, and emerging threats. The Journal aims to publish articles by authors who have professional or academic research experience with the subjects of their writing to better give insight into corporate security. Professional experience from prior military or government service is also acceptable as a means to bring important ideas from related fields to corporate security.

Topics for the Journal include but are not limited to:

- Close Protection
- Red Teaming
- Security Failures
- Intelligence Analysis
- OSINT
- Emerging Technology
- Due Dilligence
- Event Risk Management
- Enterprise Risk Management
- Security Operations Centers
- Political Risk
- Skill Development for Security
- Surveillance/Counter-Surveillance
- Private Security History

Submission Instructions

Please submit your articles to the Editor-in-Chief Dr. Treston Wheat at treston.wheat@ips-board.org as a .doc or .docx attachment by the deadline. Include a short biography about yourself to describe your qualifications to write on the subject of your article.

Please contact Dr. Wheat with any questions that you might have.