EXECUTIVE TARGETING

ANALYSIS INTO THE PROTECTION OF CORPORATE BUSINESS LEADERS

FOREWARD

As many of you know, I am a student of protection history. As Sir Winston Churchill said, "The farther back you can look, the further forward you are likely to see."

When we started The Center for Protective Intelligence (CPI) we wanted to share strategies and best practices, insights on current and historical trends, and lessons learned from physical security peers and industry experts.

In the protective intelligence space, I've always been a big believer that the how is more important than the why. The how (or tick tock of the attack) is what saves lives. I leave the why (or motive) for the analysts to ponder and debate.

Protection has evolved greatly over the past thirty years. Executive protection in particular is one that's seen a dramatic shift. Recently, the Center received a well-researched and insightful study from a Fortune 50 technology company. The company has a very mature protective intelligence and executive protection team and chronicles a look back at 18 years of threats and attacks, specifically targeting corporate business leaders. The analysis provides unique and fascinating data into the challenging job of protecting executives from both the cyber and physical security space.

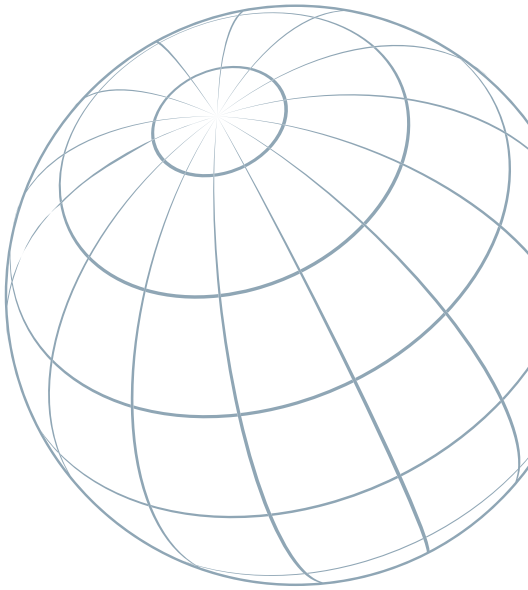
As the transformation of protection continues to accelerate, it's crucial to have thought provoking research like this that allows us to better understand trends and tactics.

The originators gave the Center permission to repost for the benefit of our industry. If there is anyone else interested in contributing content that you believe helps advance the practice of protective intelligence, we welcome your contributions.

Fred Burton

FRED BURTON
Executive Director, Center for Protective Intelligence

TABLE OF CONTENTS



OVERVIEW

The purpose of this research is to provide insight into historical attacks on corporate business leaders and trends within these incidents to increase Protective Intelligence and Operations (PIO) analysts' situational awareness. These findings can help teams gain a better understanding of the current threat landscape to executives and the changes in threats throughout the past 18 years.

METHODOLOGY

This research identifies physical and cyber attacks and incidents to corporate business leaders worldwide from January 1, 2003 to July 15, 2021 through open-source research. A diverse set of variables were recorded for each incident, such as details regarding the executives attacked, the incident location, and the assailant demographics. The data was collected through open-source research using Boolean techniques to find public reports of attacks on executives. Due to the limitations of open-source, there are likely other incidents of executive targeting not included in this data.

It is important to note both physical and cyber attacks are included in this dataset. Physical attacks or incidents represent events such as kidnappings, violent and non-violent protests, armed robbery, home invasions, shootings, and arson. Cyber incidents include CEO impersonation, business email compromise, cyber stalking, emailed death threats, social media account and phone hacks, and online terrorist propaganda.

EXECUTIVE SUMMARY

EXECUTIVES

- Male CEOs are the most common targets of attacks
- Tech and financial industry executives were targeted the most
- 40% of executives were injured or killed as a result

ASSAILANTS

- Most assailants were strangers to the executives they targeted
- The most common motive was financial gain
- Over one-third of assailants were armed with a gun or knife

INCIDENTS

- There are a total of 206 reported incidents, with 86% being physical attacks and 14% cyber-related
- More than half of incidents occurred in the Americas region
- 15% of incidents took place while on executive travel

BY THE NUMBERS

INCIDENTS

206 TOTAL INCIDENTS

86% OF ATTACKS WERE PHYSICAL

57% OF INCIDENTS OCCURRED IN TARGET'S HOME CITY

56% OF INCIDENTS OCCURRED IN THE AMER REGION

46% OF INCIDENTS OCCURRED IN THE UNITED STATES

39% OF INCIDENTS OCCURRED DURING THE DAY

23% OF INCIDENTS WERE PROTESTS

15% OF INCIDENTS OCCURRED WHILE ON TRAVEL

DEMOGRAPHICS

85% OF EXECUTIVES TARGETED WERE MALE

74% OF ASSAILANTS WERE STRANGERS

69% OF TARGETS WERE CEOs

40% OF EXECUTIVES WERE INJURED OR KILLED

37% OF ASSAILANTS WERE ARMED

23% OF EXECUTIVES WERE IN THE TECH INDUSTRY

16% OF EXECUTIVES HAD EP OR SECURITY IN PLACE

16% OF ASSAILANTS WERE EMPLOYEES

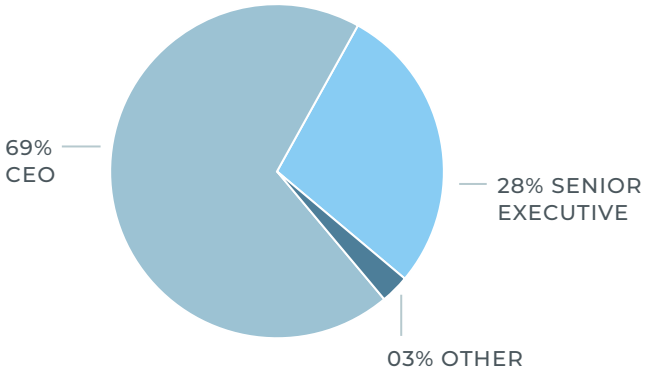
EXECUTIVE DEMOGRAPHICS

Data from open-source sites reveals targets were most commonly American male CEOs, and at least one-third of executives did not have executive protection (EP) present when attacked. Senior executives, which included any C-Suite executives and other high-level individuals such as senior directors and managers, accounted for 28% of targets.

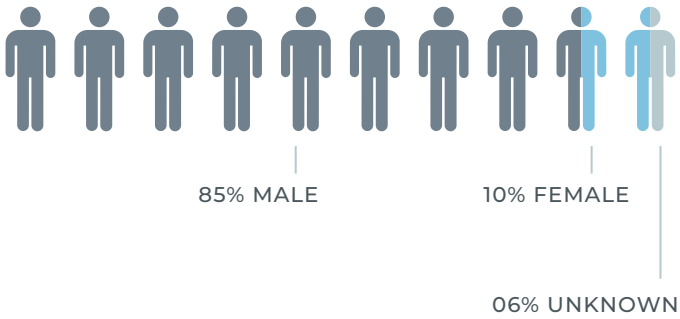
Half of the targeted executives were American (52%) and the next most common nationalities were British (5%) and Indian (5%). While the information regarding EP at the time of attack is sparse, it was found that 16% had some type of physical protection such as drivers, close protection, or CCTV at the residence.

Executives in the tech, financial, and entertainment industries made up 50% of the targets.

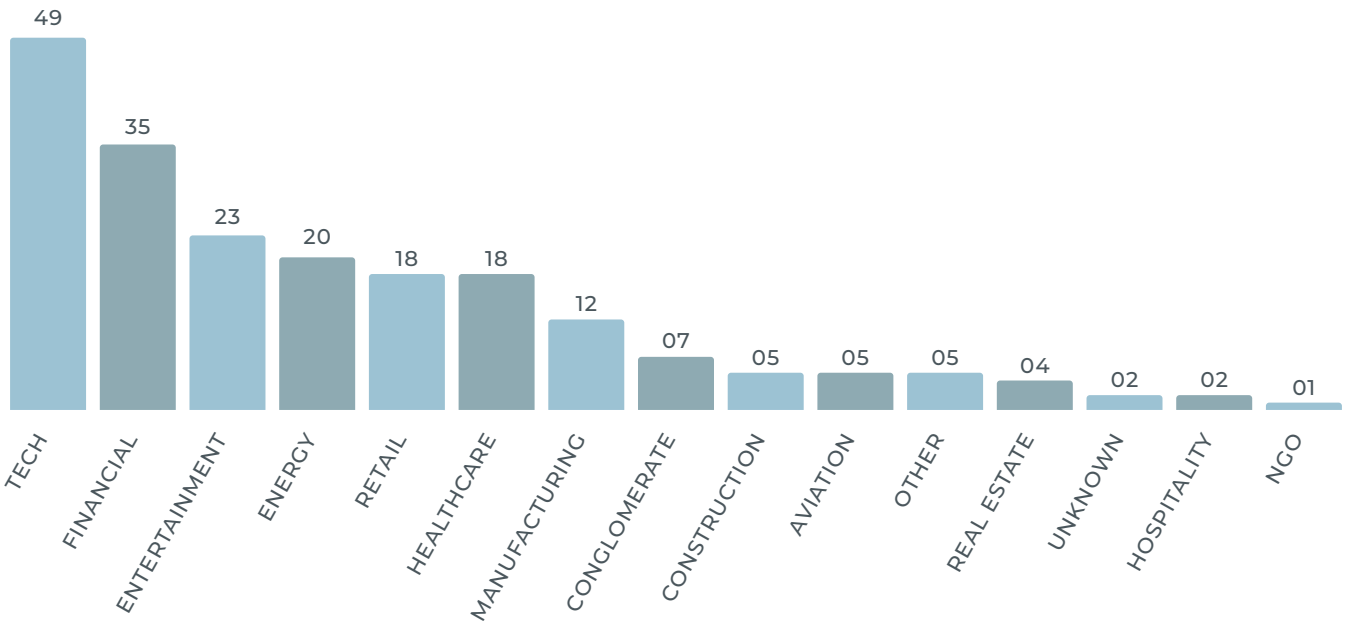
EXECUTIVE TITLE



EXECUTIVE GENDER



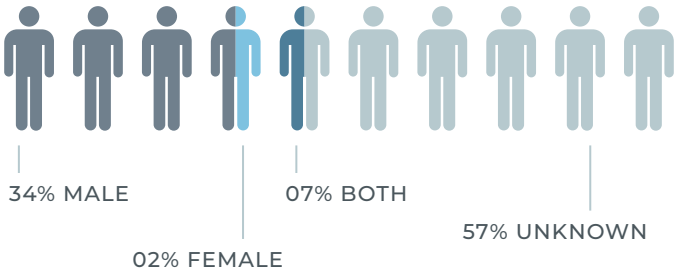
EXECUTIVE INDUSTRY



ASSAILANT DEMOGRAPHICS

Information on the assailants, those who carried out the attacks, were not as widely available compared to executive characteristics due regional reporting standards and the lack of criminal apprehension. In most incidents with available data, the assailant was male and a stranger to the executive. While most of the assailants' genders are unknown, one-third were male, 2% were female, and 7% included groups of both males and females.

ASSAILANT GENDER



The majority of assailants were strangers to who they targeted, while other common relationships included current, terminated, laid-off, or former employees. There were four cases in which an executive's EP team knew of the assailant from emails and voicemails he or she sent the executive. In these cases, the assailant typically began with cyber stalking which then led to physical stalking.

Generally, in non-protest related incidents, attacks were carried out by one perpetrator. Assailants' ages ranged from 15 to 75 years old, and many of the assailants were between the ages of 20 to 30. Groups, typically consisting of two or four people, were mostly comprised of younger individuals between 20 to 30 years old.

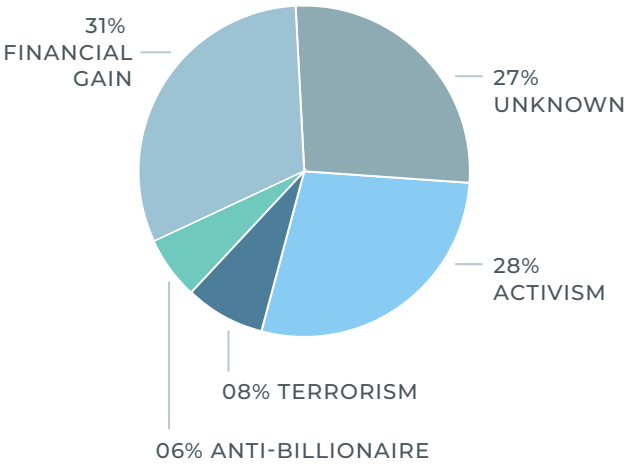
Over half of all assailants had a financial or activism related motive. Most recorded incidents are categorized as criminal, and these incidents were typically carried out for financial gain. Incidents involving activism included topics such as the environment, animal rights, politics, and religion. Activists held mostly non-violent protests, with only a few turning violent.

INCIDENT TYPE

CRIMINAL	60%
ACTIVISM	30%
TERRORISM	10%

Another common theme of protests was anti- billionaire sentiment. Additionally, there were 20 terrorism incidents, with nine of them carried out by ISIS targeting Western business executives. Incidents involving terrorism mostly included cyber tactics of propaganda and death threats via mail, email, and Twitter.

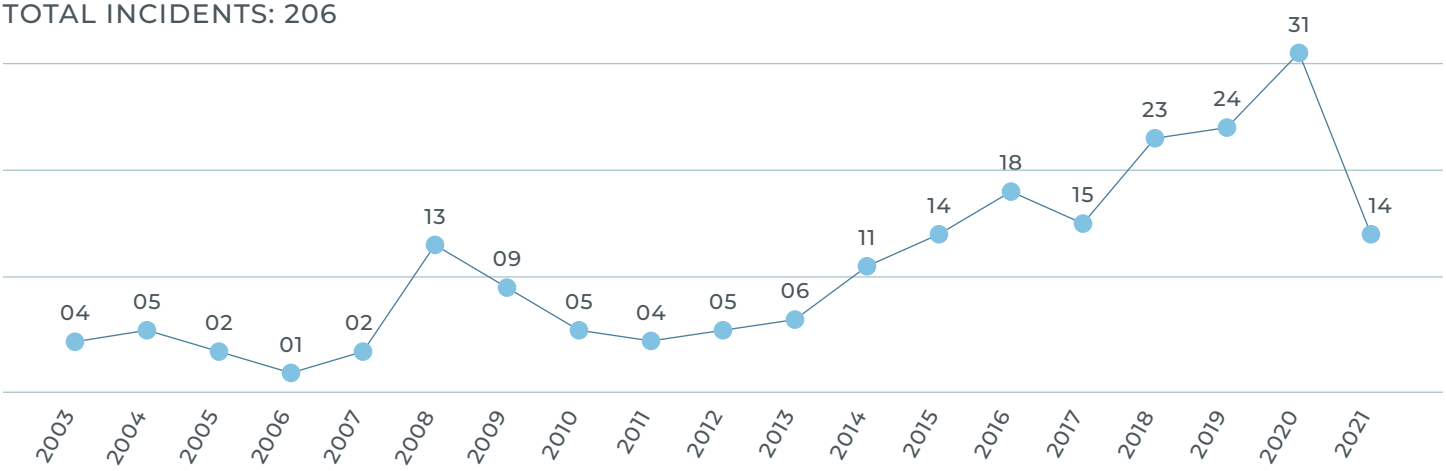
TOP 5 MOTIVES



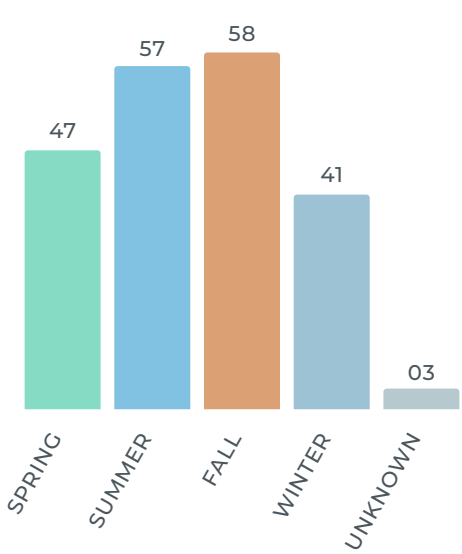
INCIDENTS: OVERVIEW

Using open-source research techniques, a total of 206 attacks on executives from January 1, 2003 to July 15, 2021 were identified. 2020 saw the highest number of incidents at 31. Half of these incidents were protests, and eight of those were related to COVID-19 working conditions or protesting billionaires during the pandemic. Breaking the years down into business quarters and seasons, attacks occurred mostly in the summer and fall months, which correlates with high numbers in Q3 months, August through October.

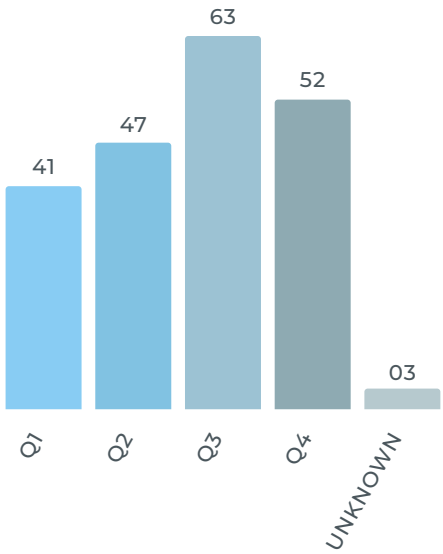
TOTAL INCIDENTS: 206



ATTACKS PER SEASON



ATTACKS PER QUARTER



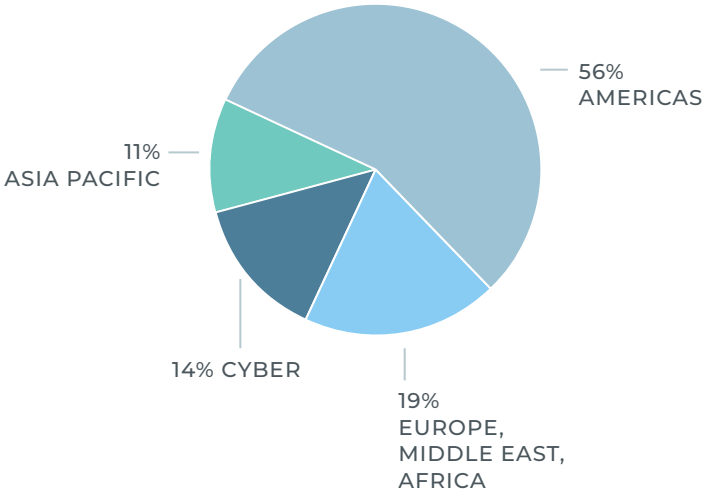
INCIDENTS: LOCATION

Based on location data, attacks were most common in Western regions, such as the Americas and Europe, Middle East, Africa. Over half of all incidents occurred in the Americas region, and 47% took place in the US. The most common cities in the US where executives were targeted were San Francisco, New York City, Dallas, Washington, D.C., and Los Angeles. Within Texas, a total of six incidents occurred in Dallas, one in Houston, and one in Arlington, with no reports of attacks in Austin. Nine incidents took place in New York City, and no attacks were reported in Hawaii. Over half (57%) of attacks took place in the executive's city of residence.

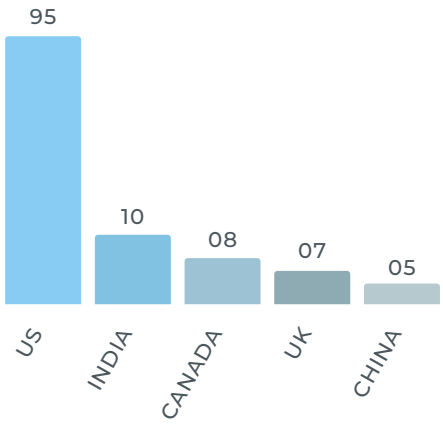
When comparing incident setting, almost half (44%) of the attacks took place at an executive's primary residence, 41% occurred in a public setting, and 14% were cyber incidents not geographically bound. Common public settings included vehicles, walking on a street, events such as shareholder meetings and conferences, and workplaces.

Half of the executives attacked (55%) were not traveling at the time of the incident. Only 15% of these attacks took place during executive travel; however, it is unknown for 15% of the cases whether the executive was on travel or not. Incidents that are not applicable (N/A) refer to cyber incidents.

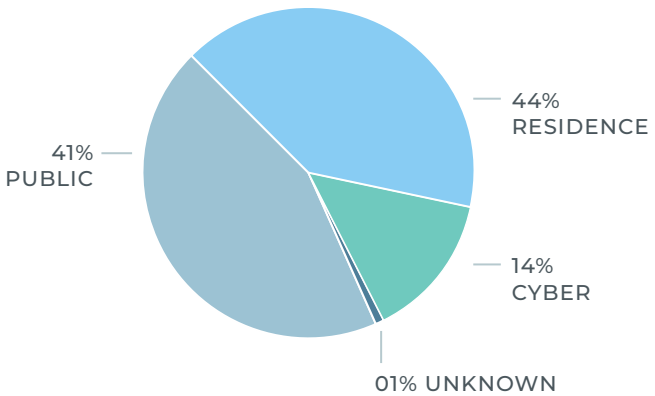
REGION OF INCIDENT



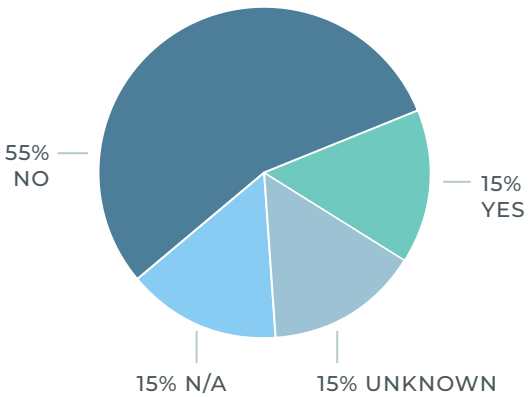
TOP 5 COUNTRIES



PRIVATE VS. PUBLIC



ON TRAVEL



INCIDENTS: PHYSICAL

Looking only at physical incidents, protests were the most common form of targeting, especially in the past five years. The second most common was shootings, which typically occurred at a residence and as drive-by shootings. Kidnapping, specifically kidnap-for-ransom, was third most common. Regarding tactics used to carry out these attacks, ambush was the most common tactic used for shootings, kidnapping, and other physical attacks. Non-violent protests were the second most common tactic, and third was home invasions, which were used for kidnappings, shootings, physical attacks, armed robbery, theft, and stabbings.

There are no consistent trends or patterns regarding the time of day in which these attacks took place besides protests usually occurring during the day rather than at night.

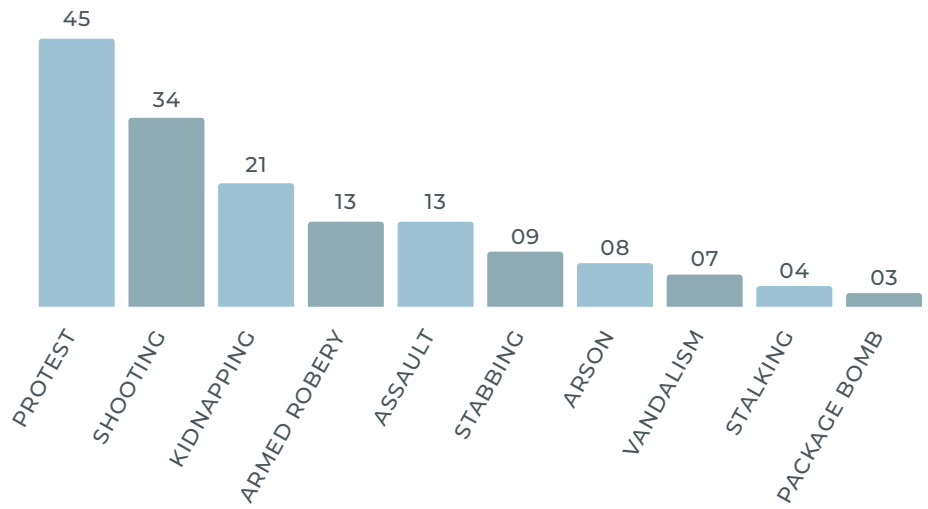
Data reveals 49% of the total incidents did not result in any physical injury to the executives. However, one-third (40%) of all attacks resulted in an executive casualty, and 7% in physical injury. Shootings most commonly led to the death of an executive. The second most common impact was disruption, which included all protests at residences and events.

It is important to note that information regarding impact to company stock, especially following an executive death, was not readily available or included in public news reports.

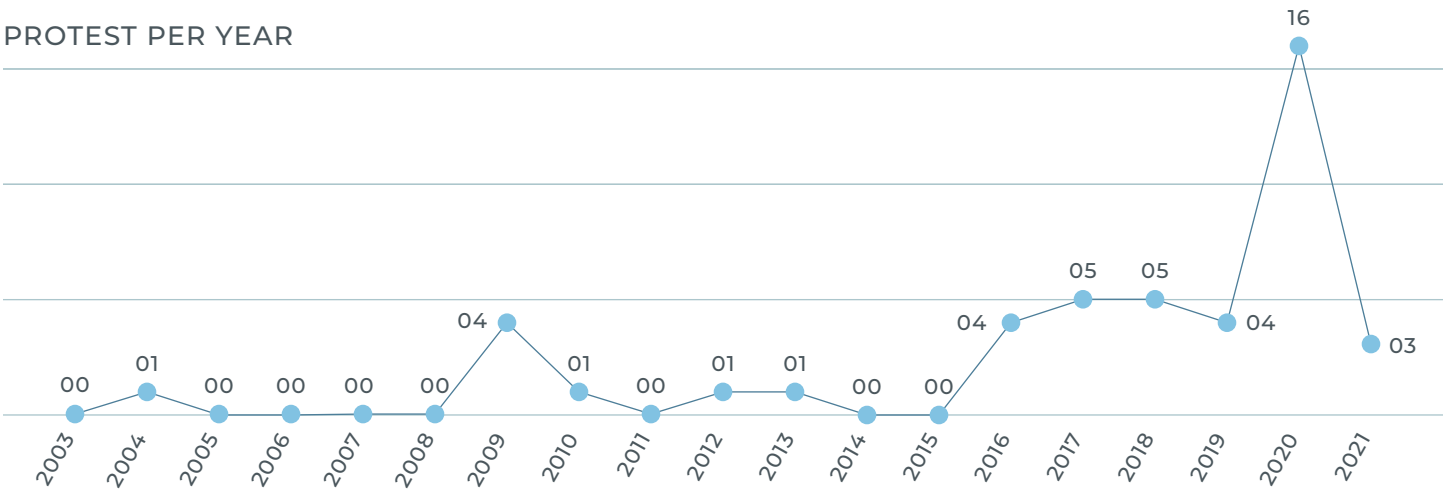
IMPACT OF ATTACK

DEATH	33%
DISRUPTION	25%
NONE	11%
PROPERTY DAMAGE	08%
INJURY	07%
MONETARY LOSS	06%
N/A	05%
EXEC TERMINATED	01%
DATA COMPROMISE	01%
UNKNOWN	01%

TOP 10 INCIDENT TYPES



INCIDENTS: PROTESTS



Protests have become a more common type of executive targeting incident in recent years. There have been at least four protests per year since 2016, and already three in the first half of 2021. From 2003 to 2015, there was a total of eight protests. Almost three-fourths of protests took place at an executives' residence and were non-violent. Non-violent protestors usually stood outside an executive's residence or event with signs. Four percent of protests caused property damage and disruption at executive's residences. Other locations where protests occurred included conferences and events (14%), shareholder meetings (6%), and worksites (2%).

CEOs in the tech industry are being targeted more in recent years. This could be due to larger, more well-known companies, and their executives being in the public eye more so than other industries like healthcare or retail. The most common motives for protests specifically targeting tech CEOs are anti-billionaire sentiment and political affiliation/influence.

73% OF PROTESTS WERE NON-VIOLENT AND OCCURRED AT AN EXECUTIVE'S HOME

CEOs IN THE TECH INDUSTRY ARE BEING TARGETED IN PROTESTS MORE IN RECENT YEARS COMPARED TO OTHER INDUSTRIES AND EXECUTIVES.

INCIDENTS: CYBER

In addition to physical attacks, there were 28 cases of cyber-related incidents targeting executives. The two most common types of incidents were death threats and CEO impersonation. Death threats were most commonly sent via ISIS propaganda targeting Western executives. Other threats were sent via email or posted on Twitter. Ten out of 11 cases of CEO impersonation involved business email compromise (BEC), a cyber crime in which a hacker commits email fraud to target an individual and their access to a company or organization. In all 10 cases, this tactic was used for financial gain in which the cyber criminal posed as an executive and sent a legitimate request to another employee at a company for banking information or payment, which was intercepted by the fraudster. The other case of CEO impersonation involved the use of artificial intelligence to mimic a CEO's voice, and the motive was financial gain as well.

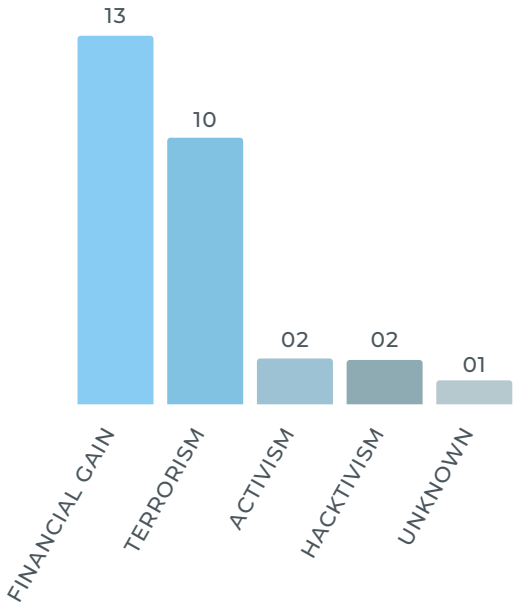
SPEAR-PHISHING

Another type of cyber attack that commonly targets large businesses and executives and that is not included in this data is spear-phishing. Spear-phishing involves sending emails purporting to be from reputable companies or executives to induce individuals into revealing personal information, such as passwords and payment information. In 2020, cyber crime group PerSwaysion sent phishing emails to executives at companies worldwide with the goal of tricking high-ranking executives into entering Office 365 credentials on fake login pages.[1] The group was successful in breaching the email accounts of high-ranking executives at more than 150 companies. Unlike physical attacks, cyber attacks involving phishing do not target one specific executive but rather a large group.

CYBER INCIDENT

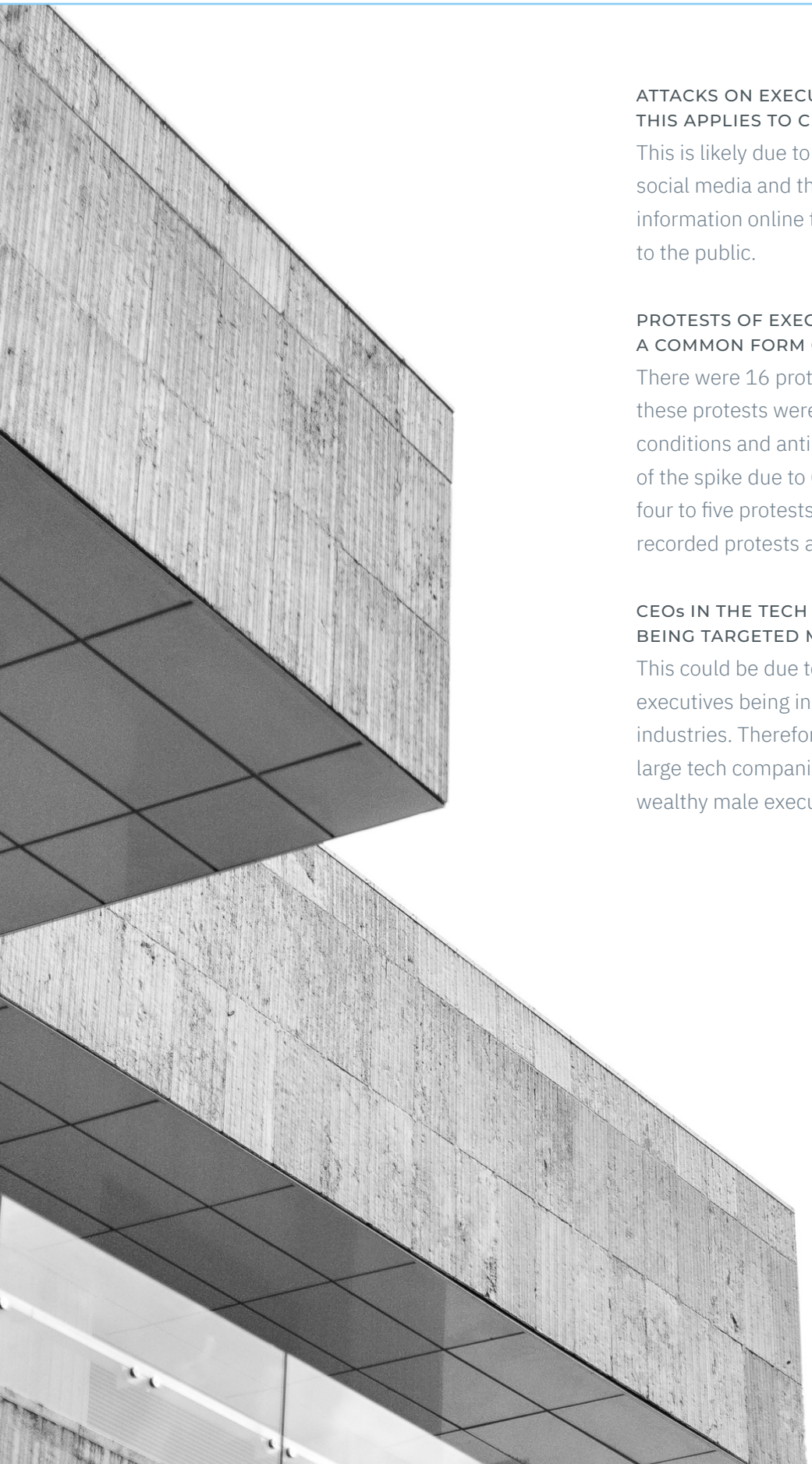
DEATH THREAT	12
CEO IMPERSONATION	11
STALKING	02
STOLEN DATA	01
ACCOUNT HACK	01
PHONE HACK	01
TOTAL	28

MOTIVE



[1] Cimpanu, Catalin. "Spear-phishing Campaign Compromises Executives at 150+ Companies." ZDNet. April 30, 2020

CONCLUSION



ATTACKS ON EXECUTIVES ARE INCREASING, AND THIS APPLIES TO CEOs AND SENIOR EXECUTIVES ALIKE

This is likely due to growing access to the internet and social media and the sharing of executives' personal information online that makes them more accessible to the public.

PROTESTS OF EXECUTIVES HAVE BECOME A COMMON FORM OF TARGETING

There were 16 protests in 2020; however, half of these protests were related to COVID-19 working conditions and anti-billionaire sentiment. Regardless of the spike due to COVID, there has consistently been four to five protests each year since 2016, with three recorded protests already in the first half of 2021.

CEOs IN THE TECH INDUSTRY ARE BEING TARGETED MORE IN RECENT YEARS

This could be due to well-known companies and their executives being in the public eye more so than other industries. Therefore, EP is particularly important for large tech companies with large, global footprints and wealthy male executives.