The Complete Collection on Protective Intelligence

Brought to you by

The Ontic Center for

Connected Intelligence

Table of Contents

The COVID-19 pandemic brought unprecedented chaos on a global scale. Even though the initial shocks of the pandemic have passed, the increased tempo of global threats and risks has not abated. For corporate security professionals, the pandemic uncovered and accelerated trends we've been managing for several years, most specifically including the 24-7 unrelenting flow of global threat information, escalating insider threats, soaring adoption of new business technologies, and an increase in threats uncovered within the digital realm.

At Ontic, we call this idea "permacrisis." Corporate security teams have dealt with problems beyond physical security concerns for many years. But in an era of permacrisis, where persistent threats from many directions have the potential to disrupt business operations and pose serious safety and security concerns across the organization, corporate security teams must adopt new methods and tools to address the increased tempo of threats and promote resilience and adaptability within all areas of the business.

Our work at the Ontic Center for Connected Intelligence centers around three key principles:

1. Hostile actors are likely to leave evidence of their intentions.
2. The Protective Intelligence framework empowers organizations to detect hostile signals, enabling them to take action to manage risks and protect their personnel, assets, and business operations.
3. Technology should not replace trained operators, yet should be used as a force multiplier within the Protective Intelligence process, substantially improving an organization's ability to find and analyze signals and sift out noise.

The collected works in this book distill how corporate security professionals can think about these ideas and implement the Protective Intelligence method in their programs. These strategies can help your teams create more holistic and mature methods for managing risks, moving beyond a traditional "guns, guards, and gates" mentality and creating more mature risk management programs that can address a wide variety of concerns, like health and safety, travel security, information security, executive protection, and supply chain security.

In the first section, we'll define Protective Intelligence and give some concrete ideas of how the process can detect and interrupt hostile actors in progress. Next, we'll examine ways corporate security teams can implement Protective Intelligence principles into their programs, including methodologies like threat assessment, surveillance detection, travel security, and building effective corporate security teams. Then, we'll look at how technology can be used to support Protective Intelligence programs, providing best practices and lessons learned about implementing new tools on your team. Finally, we've included several case studies of incidents prepared by The Center to demonstrate how Protective Intelligence practices could have been used to intercept attackers in several high-profile cases.

We hope the ideas presented in this book can help practitioners think more holistically about their programs and implement Protective Intelligence methods using industry best practices. In our years working in both the public and private sectors, we've seen these principles transform corporate security programs and pay dividends regarding safety, security, and the bottom line. The time to implement these programs has never been better with introducing new technology tools that can augment the efforts of analysts and security managers, ensuring corporate security teams have "always on" information collection and analysis to protect your organization.

After you finish this book, we hope you'll join the conversation at The Ontic Center for Connected Intelligence at www.ontic.co/center, where we regularly post new whitepapers, case studies, podcasts, and other resources to help security practitioners understand the threat environment and keep their people and operations safe.

Tom Kopecky

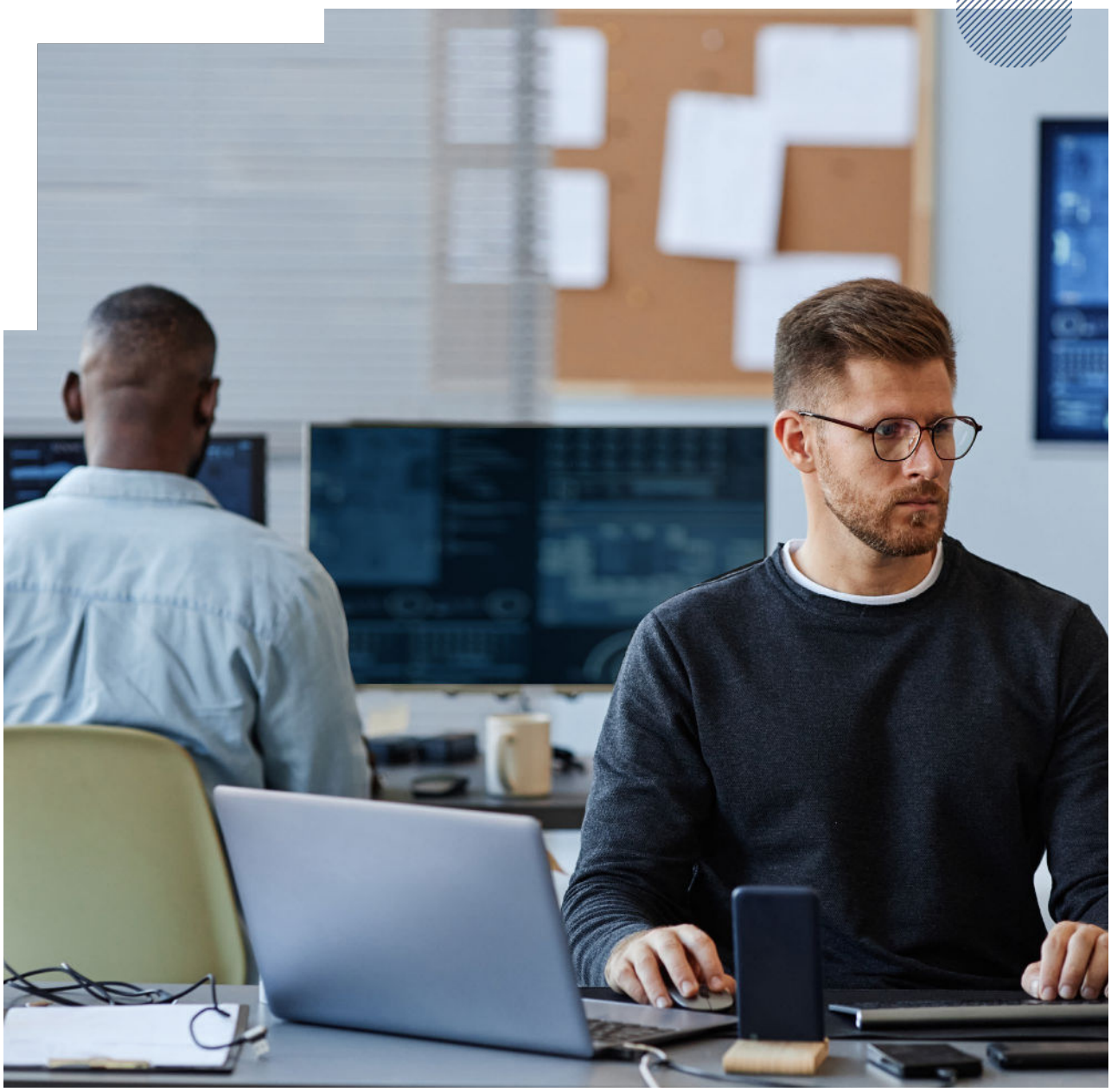
Fred Burton

Chuck Randolph

Anya Alfano

SECTION I

Protective Intelligence Defined



What is Protective Intelligence?

By: Tom Kopecky

To the security intelligence analyst plugging away in a 24-hour operations center, Protective Intelligence is one thing. To the security consultant with an MA or MS in psychology, Protective Intelligence means something else. And to the United States Department of Justice or the U.S. Secret Service, it takes on another meaning.

While the term Protective Intelligence is not used every day in an average security professional's vocabulary, it is the most defining element of a program's success in being proactive rather than reactive. It can be defined as:

Protective Intelligence is an investigative and analytical process used by protectors to proactively identify, assess, and mitigate threats to protectees.

In Security Weekly's article, "The Proactive Tool of Protective Intelligence," authors Fred Burton and Scott Stewart share their definition:

> "In simple terms, [Protective Intelligence] is the process used to identify and assess threats. A well-designed [Protective Intelligence] program will have a number of distinct and crucial components or functions, but the most important of these are countersurveillance, investigations, and analysis."

However, understanding the potential threat is essential to implement an effective security program. Structuring a Protective Intelligence program because others in the industry are doing it is not enough. Knowing the threats you're facing should be the "center of gravity" for your security program.

Breaking "Protective Intelligence" into Digestible Components

Now that we understand the Protective Intelligence definition let's walk through the full process, phase by phase:

Identify: How Do Protective Intelligence Teams Identify Threats?

The most fundamental step in identifying threats to key assets/personnel is conducting a thorough risk threat vulnerability assessment (RTVA). This allows the organization's entire security apparatus to implement proactive measures at various levels and quickly share information before a threat materializes. They can see through the noise to know what to act on and when. As Fred Burton shares in his October 2020 Security Magazine article, "The ability to see around corners has never been more important." In addition, it makes it easier to know where threats are and where they're being directed so resources can be allocated efficiently.

Once a Protective Intelligence threat assessment has been conducted and appropriate security measures are implemented, the Protective Intelligence team may rely on security and non-security staff observations. These may include any combination of the following, as an example: static security staff, counter-surveillance personnel, executives, executive assistants, household staff, corporate security staff (other than executive protection), and more.

This leads us to one of the biggest obstacles in the Protective Intelligence process: data. What types of data do Protective Intelligence analysts need to collect, and how can they store it for current and future analysis?

When it comes to proactive threat management, there is no shortage of data to assess. All of the information the security team comes in contact with is valuable data — from security officer reports to person of interest (POI) descriptions, field observations (including vehicle descriptions), written communications directed at protectees, and more.

However, Protective Intelligence is only as valuable as it is available and accurate. Security teams need the ability to retrieve data quickly on past incidents or POIs to avoid the all-too-common reactionary approach. The best way to do this is to use a software platform that leverages a database of information, allowing teams to:

1. Accurately assess the behavior of POIs over long periods of time
2. Reliably capture information for potential litigation (or law enforcement action) against POIs
3. Collect hard performance data to support security program effectiveness
4. Identify trends and patterns over time

Assess: Are They a Threat, or Not?
Security practitioners begin the assessment and management process by outlining their research, which can be summarized in a short series of questions:

- **The problem:** What does the executive protection manager need to know? (ex: Threat level of POI and recommended action)
- **Data collection:** What additional data is needed, where can it be collected from, and how can it be collected efficiently/systematically?
- **Data analysis:** What hypotheses can be supported or discounted given the data?
- **Report preparation:** What report structure does the consumer (executive protection manager) prefer?

After the case is outlined and inputs from the Threat Identification Phase are factored in, the investigation can begin. To bring color to the threat(s) in need of attention, Protective Intelligence investigations may include (but are not limited to) any of the following:

- Security officer reports/chronologies
- Human resources reports
- Open source intelligence (OSINT) research
- Proprietary database research
- Consultation with psychology professionals

Mitigation: What Strategy Will Create the Safest Outcome for the Protectee?
After the assessment phase, the security team should have sufficient support for why or why not the POI is a threat and to what degree. Now, the decision-makers can use that information to decide on the preferred course of action that will produce the safest outcome for the protectee.

Here's the catch: A security program may have 5, 10, 20, or more active threat cases to monitor at any given time. How does one allocate resources to track active threat cases, and by what systematic process are active cases reassessed?

Finding a software platform that surfaces alerts according to priority level is one way to help. It is an example of how technology has freed up space for security teams to be the eyes and ears of the company, providing intelligent security protection versus being buried in data.

For Protective Intelligence teams, monitoring and reassessment are an ongoing process. Monitoring, also called threat tracking, can take many forms — from social media to physical surveillance to third-party monitoring programs. There is often no clear-cut indicator for when a particular threat case can be put to rest. It will depend on the judgment of those who know best — Protective Intelligence analysts and leaders.

Personal Observations on the Evolution of Protective Intelligence

By: Fred Burton

Author's Note: Thanks to Scott Stewart and Mike Parks, Protective Intelligence professionals who were with me in the trenches from the beginning and contributed to this article.

The Protective Intelligence model was developed and implemented by the U.S. Government to support protective operations. In 1998, we transitioned the model into the private sector, and it is now deemed among the "best practices" in protecting CEOs, corporations, and executives.

The Backstory

In the 1980s, I was fortunate to have been part of the original unit in the State Department's Diplomatic Security Service that recognized the need for Protective Intelligence and outlined my time there in my memoir, Ghost (Random House, 2008).

In sum, we always did a good job of investigating attacks around the globe, but investigating attacks never prevented the next incident. In the 1980s, the tempo of attacks was relentless, including horrific embassy bombings, hijackings, and kidnappings. Operationally, we were global smoke-jumpers, one day in Madrid and the next in Bangkok, investigating threats and terror attacks. That high tempo of attacks against diplomatic targets began in the 1970s with the kidnappings, hostage-takings, and murders of our diplomats in Beirut, Khartoum, Kabul, Islamabad, and Tehran.

There was one constant in breaking down terror attacks – the threat actor always studied the target before attacking, a concept called pre-operational surveillance. In the same timeframe, we began training in counter-surveillance (CS) – looking for the threats outside the protective bubble by identifying anyone attempting to conduct pre-operational surveillance.

Our logic was simple: if we could identify the threat actors while the adversary was conducting surveillance, which in those days usually meant watching by foot or from a car, we could interdict or disrupt the attack cycle. One of the more interesting aspects of our CS development was recognizing that certain aspects of surveillance detection used to identify hostile intelligence services actions could be applied in the field of protection, like blending into the environment, cover for action, looking for behaviors such as lurking, photography, and time and distance variables.

Counter-surveillance became the key ingredient for the foundation of Protective Intelligence. Ultimately, we were creating concentric rings of security, pushing the security perimeter outside the physical structure of the building or the protective detail. In principle, the concept is simple. But in practice, it takes training, the right team members, acute observation skills, and the ability to blend into the landscape. Our agents didn't wear suits and Ray-Ban sunglasses. They were dressed down in street attire and blended into their surroundings. Some were bike messengers, and others sat at bus stops. It was a lonely job.

When Mike Parks of our unit wrote the first memo explaining the concept, our operating premise to sell the idea was entitled "Protective Intelligence Counter-Surveillance or PICS." PICS became the acronym. When we rolled out our first teams, the agents' radio chatter referred to the CS team as "pixies" because we were out of sight and would mysteriously appear, but we were always watching their backs for trouble. (Of course, "cop humor" might also have been behind the nickname, but either way, I think we earned our keep.)

The Early Days

In the United States, two federal agencies were at the forefront of the concept of Protective Intelligence and threat analysis: the U.S. Secret Service and the State Department Office of Security, known as SY. In the 1960s and 1970s, tragedy forced change for U.S. Government agencies driven by Congress and various Congressional investigative commissions responding to political assassinations, terror attacks, kidnappings, and bombings.

For example, the Warren and Inman Commissions changed the operational landscape for both organizations for decades. Other U.S. Government agencies have Protective Intelligence teams, including the U.S. Capitol Police. The Los Angeles Police Department has long been recognized as having a tremendous threat assessment group focused on celebrity stalkers.

At the time of the Kennedy assassination, the main job of the USSS Protective Research Section (PRS) was to collect, process, and evaluate information about persons or groups who may be a danger to the President. PRS was small, comprised of 12 specialists and 3 clerks. The unit was responsible for creating "flashcards," 3×5 index cards that depicted persons of interest. Protection agents carried the flashcards in their suit pockets and studied them during downtime. The agents memorized the faces of the BOLOs or persons of concern, as former special agent Jerry Blaine from the Kennedy detail told me. As one can imagine, this must have been a daunting task.

The Secret Service PRS team also kept detailed manual records on persons of interest (POI) since the historical threats directed towards the President of the United States came from lone shooters, like Lee Harvey Oswald, Squeaky Fromme, Charles J. Guiteau, Leon F. Czolgosz, Sarah Jane Moore, John Schrank, and Guiseppe Zangara. Interestingly, except for Oswald, very few had a history of violence, as the Warren Commission noted.

The State Department's SY/TAG unit had a similar mission but focused on terrorist groups, such as the Black September Organization. In December 1976, the SY Threat Analysis Group (known as TAG) was created within the Department of State, along with the SY Command Center, driven by the March 1973 hostage-takings and killings of Ambassador Cleo Noel and Deputy Chief of Mission Curtis Moore, along with a Belgian diplomat, at the Saudi embassy in Khartoum, Sudan.

The Modern Days

After the bombings of the U.S. embassies in Beirut and Kuwait, SY became the Diplomatic Security Service in 1985, and the Counterterrorism and Protective Intelligence (PI) Division was created to supplement the Threat Analysis Division with an investigative approach. The unit was based out of headquarters but operational in the field. Its primary mission centered on intelligence, threat briefings, threat investigations, counter-surveillance, supporting protective operations, special events, and the Secretary of State's international trips. Early protective details included the Middle East Peace Conferences, United Nations General Assemblies, visits of foreign dignitaries like Mikhail Gorbachev, PLO Chairman Yassir Arafat, the British royal family, and the Olympics in Atlanta.

Even in the early 1990s, warnings to "Be on the Lookout" – also known as BOLOs – of persons of interest were typed, photocopied, and passed around by hand. The process was very similar to how the LANCER detail operated when it protected President Kennedy in the early 1960s.

The Secret Service has always been recognized as the gold standard in Protective Intelligence, especially in threat assessment and management. Integrating analysts, threat analysis, and psychologists into the management of threat cases provided a holistic approach to threat mitigation.

In 1998, the Secret Service created the National Threat Assessment Center (NTAC) to provide research and guidance into the protective mission. Also, in 1998, the Secret Service produced "Protective Intelligence & Threat Assessment Investigations: A Guide for State & Local Law Enforcement."

Protective Intelligence Moves to the Private Sector

In 1998, we transitioned the Protective Intelligence model – to include the creation of the first dedicated Protective Intelligence analyst in the industry – into the private sector in support of protection for a major technology company and its high-profile founder. Scott Stewart – now the VP of Intelligence at Torchstone Global – was the first Protective Intelligence analyst. Word spread to other Fortune 500 companies and the next thing I knew, we were explaining the concept to many others.

At its core, the Protective Intelligence approach is perfect for protecting CEOs, families, children, estates, and executives. Discreet protection is especially popular because it creates doubt and confusion among potential bad actors while giving protectees the gift of leading their lives unencumbered by obtrusive "goons with guns" style protective details. It also works very well in protecting home offices and headquarters facilities.

What we needed during that time was innovative technology to help, aside from slow GPS tracking capabilities for vehicles, which was unobtrusive and informed our protection efforts. Excel spreadsheets were our most used databases, and the investigative work was often slow, sometimes outdated, and labor-intensive.

Protective Intelligence Today

Digital technology has transformed Protective Intelligence, leaving behind the 3×5 index cards and typewriters that were once our primary tools. I like to call it holistic or umbrella Protective Intelligence now. License plate readers, image matching, continuous monitoring, crime and weather alerts, threat assessments, integrated systems, and workflows have all been transformative. The human failure of missing a signal from an observation post or gatehouse can often be eliminated using technology. Step-by-step workflows inside platforms can also help you make sense of a threat and ensure your team responds consistently. Threat actors can be databased and automatically updated with new signals and actions, including geo-fencing areas so that you can track the proximity of threats. Real-time alerts have always mattered, but now technology is truly watching your back.

Protective Intelligence is a living, evolving endeavor. At any given moment, the same technology that enhances our work is also accessible to threat actors. We have ample evidence that the more sophisticated among them use it to great effect. Look at the October 2016 home invasion and robbery of media personality Kim Kardashian by a sophisticated criminal group. The incident almost certainly used a combination of old-fashioned, eyes-on surveillance and very modern eavesdropping of her online communications to time their attack when her security was not present. Staying ahead of the technology curve is critical – the bad guys are doing it too.

What It Means To Be a Protective Intelligence Analyst

There isn't an action or behavior that doesn't matter to a Protective Intelligence analyst. The role might seem like an odd fit to outsiders since "an analyst's contributions usually look quite different from the work done by 'typical' protectors, such as law enforcement, military, or security officers," says Matthew Stouffer, Security Intelligence Analyst at a Fortune 500 automaker. He shares that "because of the level of detail at an analyst's disposal, they are often asked to answer questions that no one else within the organization can."

To highlight the lesser-known motivations and attributes that Protective Intelligence Analysts strive for each day, we captured the thoughts of three leaders in the space. Here's what we learned:

Key Insights from Successful Analysts

After asking Protective Intelligence practitioners at a leading cryptocurrency exchange what a successful day or week looks like, the following insights rose to the top of the list:

Identify What's Important Today

Finding the right answers requires sifting through the 'noise' and identifying when to jump down that rabbit hole. However, knowing when it's time to come back out of the rabbit hole and refocus efforts is just as important.

Select Resources to Inform Action

Research often involves an array of open and closed-source tools, methods, and depositories to collect critical intelligence on a person, company, event, or issue of interest to the protectee. The analyst can take all the bits of information and piece them together to fully understand the nature of the issue. This information fuels the Protective Intelligence team to make recommendations to its protectees about how to reduce inherent risks or stop an incoming threat in its tracks.

Know Your Audience

Ensure these findings resonate with "internal business units, the protectees, and other stakeholders can be as important as the work itself," says a Global Protective Intelligence Manager at a leading cryptocurrency exchange. He shares that carrying out each project and investigation with the audience in mind is proven beneficial.

Top Attributes of a Protective Intelligence Analyst

While daunting to some people, "the challenge of solving new problems every day is one of the most interesting parts of the job," shares Stouffer. The high-stakes issues analysts face daily have real-world consequences, impacting not only the company's financial success but also the employees' physical safety.

Like any profession, Stouffer shares that there's room for many different skill sets and personalities, but some overarching attributes of successful analysts include:

Resilience
Working in protective services, even as an analyst, often involves stressful circumstances and exposure to unpleasant situations and concepts.

Adaptability
A wide range of problem sets requires an analyst to quickly absorb new ideas and information. In many organizations, an analyst's job responsibilities can also change rapidly.

Critical Thinking
At the core of an analyst's job is their ability to approach a problem or question with a mix of logic, curiosity, and outside-the-box thinking — all while striving to recognize and eliminate bias from the analysis. Richard Pittenger, Intelligence Analyst for the New Jersey State Police (NJSP), shares, "As professionals, we focus on the protectees' safety, regardless of whether we agree or not with their politics."

Prioritizing Reflection and Self-Care
Above all else, the Protective Intelligence analyst role requires self-discipline to step away from the speed of changing information and take care of oneself when the time is right. "Given the long hours, constant alerts, increasing threats, low margins for error, and minimal resources, analysts are at risk for burnout," shares Pittenger. Analysts must find support to manage the chronic workplace stress compounded by personal stressors. This not only prevents mistakes but also decreases the protectees' vulnerability.

Surveillance Detection: You Can't Find Surveillance Unless You're Looking for It

By: Fred Burton

I learned surveillance tradecraft the hard way in the 1980s, as chronicled in my memoir Ghost: Confessions of a Counterterrorism Agent (Random House, 2008). History has been altered with significant Protective Intelligence failures and tragedies, from assassinations to school shootings, many caused by failing to notice or act on hostile surveillance. The sad reality is this: most victims rarely know if they are being watched until it's too late. Once the actor with ill intent has walked down the pathway toward violence and arrived at the target location, the attack is hard to stop.

For a stalker or assassin to be successful, they must study and observe their target, which makes them vulnerable to surveillance detection. The challenge is seeing the surveillance taking place.

To stop an attack from occurring, you need to disrupt the attack cycle. One of the best ways to disrupt the attack cycle is to catch the actor at the point in the attack cycle where they are most vulnerable to detection: during the pre-operational surveillance phase. Surveillance detection programs, augmented by technology, can be used to identify fixated behaviors and operational acts during the planning stages of an attack.

After a lifetime of examining successful and failed attacks, I've determined there are two critical components to understand. The first is the attacker's motive or the "why" behind the attack. The motive is important for the investigators to figure out and for analysts to ponder, but knowing the motive does little to stop an attack from occurring.

The second component is the attacker's method of surveillance and attack or the "how" behind the attack. The method and means of surveillance the attacker uses are critically important because understanding how surveillance takes place allows you to look for similar actions.

Every attacker, stalker, or criminal watches their targets, so it's important to know what those actions will look like and understand the geographic locations where you would most likely encounter them. The challenge is seeing the surveillance taking place.

Surveillance Detection Basics

So, how do you look for surveillance? First, you can't find surveillance unless you are looking for it. In concept, this is a simple and practical idea, but it is hard to know what to look for on the streets, standing post, or while protecting an estate. Technology solutions can help augment the human eye and mind, but these skills can also be taught.

When I teach surveillance detection skills, I use three key concepts:

Mindset
To start, look for things that don't fit. Study your geography, know your street, block, and neighborhood, and develop a baseline of normalcy. Once that baseline is established, anomalies will stand out—you'll notice a stranger lurking, a suspicious van, or vehicles driving slowly or perched as observation platforms. Own your geography and know what is out of place. It is also imperative not to have a mindset of complacency, with a sense that nothing can ever happen. Don't get complacent about your normal surroundings.

Observation Skills
You can learn to see better. How? Practice. Many years ago, I took a course given by one of the alphabet soup agencies that showed how much we needed to learn about observing the world around us. It was embarrassing and eye-opening (pardon the pun) for a classroom filled with special agents, security, and protection officers. The instructor flashed a quick image onto a big screen and asked us to describe what we saw. Invariably, everybody got it wrong. You can begin to get it right by practicing your observation skills in the world around you.

For example, some of the most sophisticated surveillance teams in the world once worked from rooftops, but only some people think to observe what is happening above them. Why? Humans rarely look up unless they hear an aircraft. Now, the same concept exists in drones and surveillance cameras. Observation and counter-surveillance skills take practice, patience, and awareness.

Pattern Analysis
Look for abnormal or unusual activity patterns in your everyday life, especially in locations you often visit where an attacker might try to surveil you. The key here is heightened situational awareness on your first move of the day. When you depart your residence, take a mental snapshot of the people, faces, and cars you observe. Later, if you see the same person or vehicle over a period of time and distance, you'll know someone could be watching.

Here's an example: You leave your house in the morning and see a blue van across the street. Then you drive to work. You see the same blue van outside your workplace when you leave work later the same day.

The blue van was observed over time—first during the morning departure and later in the evening departure—and distance—first at your home, then at your workplace. Nation-state surveillance teams never let you see the same person, vehicle, or bicycle more than once. Criminals or stalkers rarely have those resources, so the advantage is on your side, but only if you are looking. Once again, technology can help make sense of the behaviors captured, such as multiple surveillance drives near an estate or multiple passes over time.

Surveillance Detection Exercises

There are a few simple practices that will help you begin to hone your surveillance detection skills. One simple exercise you can incorporate into your daily routine to smoke out surveillance is called a Surveillance Detection Route or SDR. An SDR is used to determine if anyone is following or watching by using a series of simple directional changes.

Here we go. Walk or drive down Main Street, make a left on 1st Street, then make a right on 2nd Street. Stalkers or attackers will not want to lose the eye, so they will stay with you. Is anybody with you? Did you notice the same car behind you? If not, you are clean.

You can string the stair-step out over distance if you are driving or by the block if you are walking. You could be under surveillance if you see the same person, car, or bike behind you after your turns. Coincidences can happen, but not in the world of surveillance.

A second practice you can implement is improving your memory skills. Sometimes, the old-school tricks are the best ones. You can learn to enhance your memory skills by observing license plates and people. This takes practice. Start by randomly observing license plates in front of you while in traffic, then elevate your game by trying to see if you can decipher plates through side-view mirrors (hard to do). Stare at the license plate, close your eyes briefly, and you should have a mental snapshot of the numbers and letters. Keep a notepad handy, or use the voice record feature on your mobile phone.

Another exercise is to observe people and try to describe them based on the features of celebrities or well-known personalities. For example, if I say that the person looks like Tom Cruise or Brad Pitt, everybody has a mental picture of who that might be. It helps when trying to reconstruct surveillance and aids with identification.

SECTION II

Implementing Protective Intelligence

Level Up Your Threat Hunting Game – Creating Intelligence from Anomalies and Patterns

By: Tom Kopecky

Not too long ago, social media or emergency news alerts were the holy grail of early threat detection. While it's true that listening for threats in social media is effective and cannot be ignored, it is still only one type of data point among the many needed to adequately identify threats in an effective Global Security Operations Center (GSOC) or Protective Intelligence program.

With data surfacing at every angle at any time of the day, we are often asked where to start when developing a more proactive security model, including what tools to use. We are also asked how to "Threat Hunt," or, as we often say, connect the dots. Equally as important, security leaders want to know how to instill a repeatable process.

In The Protector's Guide to Establishing an Intelligence Baseline, we outlined how to implement a minimum standard and make it adaptable to your organization's unique needs. Here, we want to get more granular about some data types, or data intelligence, that we can tap into to be more effective in protecting assets.

Looking At The Holistic Picture

This heightened level of granularity involves talking about characteristics and behaviors to analyze threats. When investigating and assessing threat actors, it's not always about what the threat actor says explicitly; it's also about how often they communicate and whom their communications are directed.

For instance, if a person expresses a fixation on your protectee and posts online commentary about them directly, this can be disheartening, but that alone does not provide full context. Perhaps this person routinely seeks out executives in the tech space to create controversy and rattle cages. Some threat actors get validation by knowing they hit their mark. Occasionally, the feedback a person of interest (POI) receives comes in the form of a legal threat or an admonishment by someone in a security organization.

When managing a threat assessment involving inappropriate pursuit, unhealthy fixations, and related behaviors, there are many trends to look for. It's critical to keep the full context in mind.

Immediate examples include:

- Personalization of the communications
- The tone
- Escalating frustrations
- Indirect references to the principal
- Frequency of communications and commentary

When you observe any of these trends, it indicates that a POI is actively researching its target, signaling competency and creating an urgency for the protectors to stay several steps ahead of any action this individual may take.

We also need to pay close attention to the frequency of communications or commentary so that when these communications spike, create a pattern, or are synced with other important life milestones (anniversary of a termination, financial troubles, etc.), additional scrutiny is given to the investigation.

Moreover, if a person posts strange and inappropriate commentary, and then graduates to make direct physical approaches to the executive, we need to escalate our assessment. This indicates that the previous chatter has now evolved into action — which is an important step in the attack cycle.

What Are Your Sources for Data Intelligence?

It's important to remember that our creativity and skeptical curiosity often limit our success. We have found an abundance of readily available sources that can help surface pre-incident indicators of violence. Since we tend to have more sources of information than time to make sense of it all, we need to reconsider our methods to efficiently digest data from as many preferred sources as possible.

Below, we cover a few readily available sources, as well as some that are less obvious, which can help you uncover valuable information in your threat-hunting efforts. Stretching beyond the traditional avenues for data will allow you to turn single events and observations from field operators into actionable intelligence.

An Indicator of Threat Escalation

Imagine if you were automatically notified when another team member, department, or associate organization is working on an investigation related to the same threat actor as you are. Then you receive a notification that the other team is running similar queries or investigative research and even saving files with the same POI information.

Envision that you are assigned to the corporate security team, and someone in the executive protection group generates an internal Be on the Lookout (BOLO) report on a high-threat POI. It may be safe to assume that something occurred to kick off this notification since BOLOs are typically generated in response to an escalation or action carried out by a threat actor. Now, both teams have consistent information and can determine the level of urgency for their collective plans.

Bridging intelligence gaps is key to operational success, and in our experience, getting teams talking and sharing more intel is a huge benefit for everyone operating under the same security umbrella. The technology exists to make this part of your daily routine, and combining it with the elements we outline next can make it invaluable for staying ahead of threats.

Ditch The Sticky Notes

A large part of successfully protecting people and assets is ensuring that your team does not lose track of information that may someday become key to uncovering a threat issue. Practitioners typically build internal ad hoc processes that function adequately at a smaller scale; however, there is rarely a central source of truth or a consistent, convenient process to store and share case notes when new intelligence is accumulated. Using a unified platform to store your baseline intelligence allows you to easily measure trends and identify patterns in behavior from a threat actor.

Properly saving key data points related to field observations, images, threatening communications, and team notes can make the difference between detecting and disrupting a threat or letting one slip. It doesn't take an expert to tell you that even the smallest mistake can lead to irreparable damage.

Real-Time Access To The Facts

Every security program has access to information that can help them guide how they use security resources and efficiently address threats. In one program, this might be something done with pen and paper, only pertaining to threats that impact that individual team. Then, in other more mature programs, this likely includes a detailed database of threat information that spans multiple business units, such as human resources, executive protection, global security, and more.

The point is this: today, you already have vast amounts of information to help proactively address threats. However, this information is only as valuable as it is available and accurate. Security teams need the ability to retrieve data quickly on past incidents to identify behaviors and patterns. Sorting through data manually and requesting access to cross-departmental systems while a potential threat is active is one way to ensure lost productivity. Leveraging a database of information that's on 24/7 with real-time alerts lowers the likelihood that significant information changes will slip through the cracks and will increase a security team's ability to take proactive action.

Getting a Comprehensive View of Integrated Systems Activity

When in the office, employee badge readers, visitor management/access control systems, and CCTV networks provide a wealth of knowledge to the security practitioner. Surfaced and analyzed in one platform, this information becomes intelligence that practitioners rely on daily.

With a proactive security program and process in place, we can better detect and manage the attempted visits of a POI and broadly communicate those to teams that need to know. Insider threat management programs can benefit from being alerted to "out of norm" access to facilities or even attempted access by unauthorized persons.

Now more than ever, we are seeing great success with using license plate reader (LPR) cameras at client-owned facilities. Imagine pushing out your security perimeter even further by relying on discrete, low-profile LPR cameras that not only alert to "hot listed" vehicles associated with known POIs, but also report anomalous and volumetric activity by others.

LPR Cameras In Action

A POI drives by two of your principal locations on the same day — one of which is a corporate facility, while the other is the CEO's residence. With proper LPR camera integration, you can immediately be alerted to this activity. As security practitioners, we don't even need to know what else that person did to be legitimately concerned. We can deduce that they not only remain fixated on the protectee but have also crossed into a dangerous phase of the attack cycle — pre-operational surveillance and planning.

It's About Perspective

Think about this for a minute. We don't always have to know the content of the communication or the specific details of the incident or action that took place. Knowing that such a data point exists can tell us that something urgent is happening.

If we can get even more creative or level up our threat hunting and track the frequency of behaviors and trends, including spikes and dormancies, we can catch more and miss fewer signals.

Patterns of data points become pre-incident indicators. For example, if a threat actor has a known steady cadence of communication, and that stream suddenly becomes quiet, what does that tell us? Inversely, if a POI redlines its activity level, how does that impact our threat assessment?

When actively hunting for threats, it's easy to be overwhelmed with noise. Therefore, we recommend looking at the situations from another perspective: What threats might I be missing by focusing too much on individual details, rather than the holistic picture that those details create?

Shifting From The "Old Way of Doing Things"

When we take a macro view of our program that relies on information sharing across departments, as well as anomalies detected by smart systems integrated into our security toolbox, we can arrive at insights previously unavailable to us.

As the approach to protecting assets across all industries evolves to incorporate a more holistic view, we expect organizations to significantly increase their ability to protect their assets. Moving away from old habits of fixating on specific details rather than the complete story will allow us to glean new insights. And with the process of threat hunting growing more complex, this shift in approach can make all the difference in separating noise from an immediate threat.

The Protector's Guide To Establishing An Intelligence Baseline

By: Tom Kopecky

Protective Intelligence Pain Points

Over the years, we've recognized a significant need for more processes in place that would enable security professionals to gain a better understanding of their Protective Intelligence data. We know that organizations are fundamentally different and understand that very few have a standardized approach to Protective Intelligence—one size does not fit all. Threats are highly contextual and are based on numerous factors, including industry type, company culture, geographic areas of operation, as well as media attention focused on our organizations whether they be positive or negative.

What's more, those of us in the corporate security and executive protection space are quite often confined to the operational constraints that our principals unknowingly establish for us, with executives often inadvertently dictating the protective movements and coverage protocols for security teams. As security professionals, we must remain fluid and adapt to any environment, which happens repeatedly, with virtually no advance notice.

Let's Get Tactical

What if a client broadcasts their most important travel plans? Or the address of an executive office is released as public knowledge. What if the security team discovers that their office is easily accessible by unauthorized persons? We know many corporate campus entry points are less strict, and guests are left relatively unchallenged upon arrival. These types of conditions hamper any security team's efforts. Working without much high-level context, teams must often rely on training, intuition, and remote intelligence support. They are simultaneously asked to remain "low profile," focus on various facilitation requirements, and be ambassadors for the companies they represent.

Many teams are expected to be out front and all-knowing, identifying threats before anyone else. They are then asked to force multiply (without force-multiplying the security budget) and continue to do the heavy lifting when any issue arises—and remain completely invisible while doing so.

By addressing some of these pain points, we hope to answer two critical questions:

1. How do we as intelligence teams better support field operators?
2. How do we create an environment where field operatives drive more useful intelligence to the Global Security Operations Center (GSOC)?

To effectively address these pain points, we need to ensure that our protective security teams are:

- Speaking the same language when it comes to Protective Intelligence and early threat detection
- Communicating more effectively on the basics
- Establishing a professional baseline, or minimum standard when gathering or sharing intelligence, so that we aren't working in the blind

Defining a "Minimum Viable Process" for Protective Intelligence

At Ontic, three opportunities emerged as we worked to establish a minimum standard for gathering or sharing information.

1. We need to deliver intelligence fast.
2. We need to deliver it cost-effectively.
3. Our clients need the right amount of intelligence to make important security decisions or to deploy valuable resources.

We've found that an important security decision does not always require the most exhaustive investigative profile on every single person of interest (POI) that we encounter — many times, it requires "just enough." In the technology industry, this is what we call the "MVP," and it may not mean what you think.

Delivering a Minimum Viable Product or MVP means that as we build technology, we look to understand and solve the user's basic needs. It's trading perfection for pretty darn good. In automotive terms, you should start by building, for example, a Dodge or a Ford and then seeing where that gets you. You don't exhaust valuable time and resources to build a Ferrari—at least not at first.

To start, you ensure that the car meets the user's needs, will work as designed, and works pretty darn good. No development team wants to retroactively deconstruct a technology platform because they made numerous flawed assumptions about what the end state should look like. By focusing on building a MVP, the development team establishes the baseline from which to build future improvements.

Let us draw a parallel analogy here for the Protective Intelligence space, but let's instead use our acronym MVP for Minimum Viable Process. Currently, a standardized minimum viable process for the Protective Intelligence workflow does not exist in our industry—so we'd like to rectify that gap.

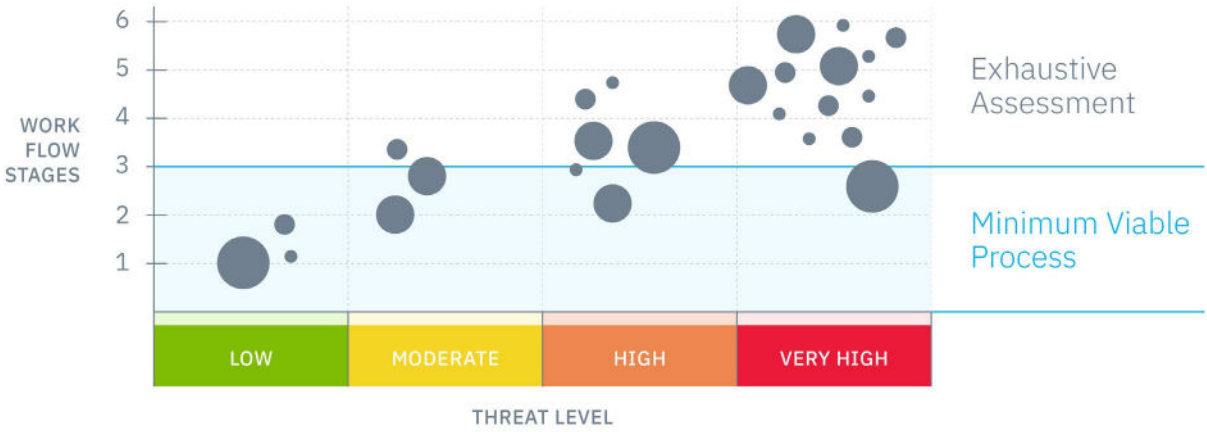
Before we built the Ontic Platform, we were asked countless times what our manual investigative process looked like. We would like to offer the following workflow that we've tested over time.

Recognizing that one size does not fit all, this isn't the definitive playbook for every team. Nor do we believe that investigations and threat assessment cases can be reduced to a checklist—gut instinct will always come into play. This workflow does, however, provide a broadly applicable baseline framework. Returning to our MVP, security teams don't necessarily need an exhaustive due diligence investigation on every single POI that appears on their radar. They simply need a foundational level of understanding of the background of potential threat actors. This prevents the waste of significant human and financial resources.

Resource-Effective Triaging of Person of Interest Investigations

All protective security teams work with limited resources (time, team size, budget, etc.). The workflow below is mindful of how we allocate time to our investigative projects: investigators should focus on each stage's outcomes, as these define success. The means we use to achieve these outcomes will always change with the situation and with the practitioner.

While we believe that the entire workflow is critical to achieving a better understanding of your person of interest data, we've defined stages 1-3 of our investigative workflow as the tactical MVP (see diagram). For a POI investigation, we consider these three stages pretty darn good to form a baseline—and should be conducted on every person of interest. These stages are defined by identity resolution, geo-location insights, open-source analysis and social media intelligence, among other criteria. It generally provides enough detail for us to assess where this POI falls on the threat spectrum—low threat vs. high threat—and what the return on our investment would likely be if we dedicated more resources to a deeper investigation. As the threat level increases, we can always choose to conduct a deeper investigation and continue on to stages 4-6 in this workflow. We believe defining these boundaries will maximize the use of finite team resources.



Workflow Stages

1. **Identity Resolution**
   In this step, the analyst or investigator must confirm who they are investigating. Example: Who is the person behind the harassing email and phone communications? Who owns the vehicle in that suspicious location near the principal's residence?

   Once we resolve their identity, we need to know what our team and associates have already discovered about that person—is there a baseline already existing on this POI, or is this one brand new to us? Do we have an initial understanding of the possible threat level based on the context of the interaction? When a security team makes an observation, how do they know what the enterprise already knows about the subject? Does human resources consider this person a serious threat due to comments he or she made in an exit interview, or does corporate security know that this subject is part of a retail crime ring? Moving forward, how do we quickly identify the person again when they surface? To do this, we must learn about the person's additional identifiable attributes, including other personal identifiers: address, registered vehicles, social handles, phone number, employment, etc.

2. **Geo Location Insights**

This step is all about location, location, location. It's simple physics—the further away from your principal or workplace a POI is, the less risk they pose for causing physical harm (there are some exceptions to this rule, of course, e.g., package bombs, chemicals mailed to a principal, IT vulnerabilities, etc.) We call this threat context by geo proximity. Is the POI on the other side of the country just making noise, or are they actively engaged in the attack cycle? Where is this person right now?

There are many sources to review and steps an analyst or investigator can take to determine where a person is at any given time. Some are quick reference searches through social media or incarceration records, while other methods include human intelligence and pretext calls, to name a few.

This step is one of the most critical because of its immediate impact on time and resources. If there's little physical distance between the POI, you may need to quickly mobilize resources. If the opposite is true, the team could relax while maintaining a vigilant posture. In essence, determining the geo-location can help a backlogged team prioritize threatening communication from a POI amongst all other tasks. For example, if it is determined that a POI is a thousand miles away from the general area of the principal, then the case can be deprioritized (for the time being) while other urgent tasks are attended to.

3. **Open Source Analysis and Social Media Intelligence**

Undoubtedly, there's a deluge of information online that can be cultivated while assessing the threat of a POI. Key issues we typically look for are mode of living, mental state, access to weapons, past behavior, fascination with violence, and fixation / unhealthy pursuit of the principal or their family. For those instances where the POI practices digital privacy, it is often easy to target by proxy and investigate the online activity of those close to them, including friends and family. We also review Deep Web forums for information related to the POI's potential affiliation with fringe groups radical ideologies, and malicious protest activity.

4. **Public Records Data**

To formulate a deeper background story of a POI, we can access public record repositories. These indexes provide exceptional access to case information, including criminal arrests, civil litigation, bankruptcies, liens, judgments, foreclosures, divorce, child custody, intellectual property, and trademark infringement claims.

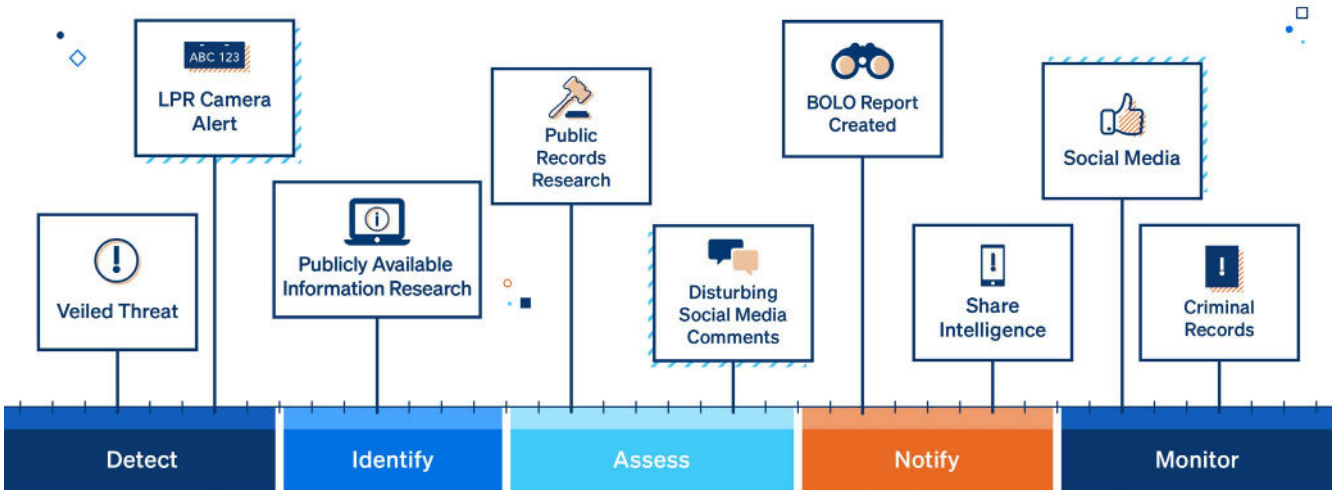
During stages 5 and 6, we move on from preliminary data gathering to more accurately assessing risk, communicating our findings with those that need to know, and implementing security protocols for that case. At this point, investigators need to get their team leadership involved to review the facts of the case and then develop a plan consistent with the culture and mission of the organization.

5. **Assess Risk Indicators, Trigger Events, and Formally Assign Threat Level**
   As analysts layer in all the information discovered in prior stages, they can make greater sense of the data points, identify potential trigger events, more formally assess risk, and prioritize other dates/events of importance for the threat actor (anniversary of termination, copycat workplace violence incidents, etc.). With this connected information at the fingertips of security professionals, they are empowered to make informed decisions about assigning a more accurate threat level to a case and move on to the next step.

6. **Develop and Implement Protection Strategies**
   There are many excellent resources about assessing potentially violent actors and developing case management strategies, such as those endorsed by the Association of Threat Assessment Professionals (ATAP Body of Knowledge). After working with corporate clients, this is our philosophy: Intelligence in a vacuum is useless, and inaction in light of it becomes a major liability.

   For example, if "Corporation A" knew a great deal about a POI who was harassing a workplace, making veiled threats, or displaying an unhealthy interest in C Suite executives and then chose to do nothing with that information— what does that say about the company's duty of care?

   When information is shared, it becomes actionable. Note: sharing information is not limited to this step of this workflow—it can and should happen throughout the process. We also find that after this much information is obtained and assessments are made, contracted professionals can be retained for guidance. For example, does this case get escalated? Does Law Enforcement become involved? Or does the corporation engage with the threat actor and their family to help the person get treatment from a trained mental health professional?



Understanding the Bigger Picture

With a holistic approach, we can now layer in all pertinent information to more accurately understand the evolution of a POI. We can even uncover potential trigger events in their life, e.g. anniversary of termination, a death in the family, or perhaps a tense legal case involving a child custody battle. By surfacing this type of information, teams can better identify a trend or anomaly in behavior and more accurately assess threat levels.

As the timeline above illustrates, a threat assessment professional can see that all of the various data points—when visually connected—create a much bigger story. Here you see the evolution of a POI:

- Subject makes a veiled threat on departure from the organization
- GSOC notices a direct threat to the brand on social media
- Campus safety notices a suspicious vehicle loitering near corporate HQ
- Public record research reveals a contentious divorce and a residential bank foreclosure
- LPR cameras detect a subject's vehicle driving past the residence of the CEO at 3:00 AM
- The security team escalates the matter, generates a BOLO report, and shares intelligence with relevant parties

What could otherwise be cataloged by siloed teams as independent events now clearly demonstrate the evolution of a serious issue.

It Takes a Community

We are fortunate to work in an industry where we typically do not compete with each other, and we can't take that for granted. We hope you will continue to collaborate with us and share your experiences. The Corporate Security Officers of competitive companies are not locked in a zero-sum game. In fact, they have much to gain by collaborating because they face nearly identical challenges, occasionally driven by identical POIs. Similarly, we encourage you to collaborate with the security communities we all participate in, such as AIRIP, IPSB, ATAP, and OSAC.

We are all in this together and, therefore should be communicating more effectively. If we can work together to proactively identify, disrupt, and, most importantly, prevent an act of violence before it is carried out, we have achieved an important victory.

Threat Assessment 101 For Corporate Security Teams

A threat assessment helps security managers and company leaders gauge risk. When done correctly, the assessment process helps to engrain specific security standards across assets and employees. In addition, threat vulnerability assessments give security managers the information they need to assign resources designed to limit and deter threats.

In a world where companies face increasing physical and cyber risks, understanding exposure and ways to improve security measures are essential to protecting assets, people, and reputation.

Learn how to build and optimize the threat assessment and management process to understand various threat landscapes. A clearer view of what's out there empowers teams to plan for and respond to security issues before they become significant problems.

Why Is a Threat Assessment so Important to an Organization?
The threat assessment is one of the most efficient tools security teams use to recognize and respond to physical security threats or information technology risks.

One of the most significant benefits of threat vulnerability assessments is they standardize the approach to threat across a corporation. In a large company, for example, security managers often have teams in different countries or use vendors as guards, supervisors, and inspectors.

Imagine a situation where each country or individual was responsible for assessing threats. Typically, people let past experiences, cultural differences, and their interpretation of risk get in the way of objective reporting. For example, how someone in India interprets crime threats will vary significantly from how someone in Singapore views crime.

A standardized threat framework changes that. It holds everyone to the same standard when assessing risks to buildings, employees, operations, digital technology, and other assets. Moreover, even standards better guarantee uniform security responses across an organization, which simplifies everything from resource management to future investment in security software.

How Different Corporate Security Programs Use Assessments
Threat assessment often broadly refers to an organization's risk measure. A site security assessment, for instance, is typically a report highlighting a facility's security measures and assessed ability to detect or deter threats. On the other hand, an investigations manager uses threat assessments to understand the impact of any threat of violence in the workplace.

Here's how different security functions use threat analysis and risk assessments.

Executive Protection
Executive protection teams are usually on the receiving end of threat assessment reports. For example, intelligence analysts, protective intel teams, or regional security managers feed information to close protection teams to keep them abreast of ongoing security threats or conditions on the ground where they travel.

Protective Intelligence
Protective Intelligence teams at large corporations typically receive threats and unwanted interactions that target company executives. As a result, they manage cases and produce reports that go to executive protection team members, security directors, and C-suite clients.

Regional Analysts
Regional or Protective Intelligence analysts create threat assessments to communicate risk across the organization in response to terrorist attacks, political unrest, social upheaval, crime, and other security conditions.

Investigations
Investigators manage cases related to everything from insider theft to workplace threats of violence. They investigate the loss of digital assets and identify retail shrinkage trends. Threat assessments help them manage resources and risks to the company.

Global Asset Protection
Asset protection teams vary, but most are responsible for protecting high-value assets like source code, formulas for food products, or hardware on display in retail locations. Threat assessments help them decide how much money to spend on cybersecurity and physical security measures to stop bad actors by protecting corporate assets.

Cyber Security Threat Assessment
Cyber security teams use network and IT threat assessments to prevent attacks against their networks and digital assets.

Aligning the Risk Assessment Framework with Corporate Values
Creating a functional threat assessment program requires a framework defining acceptable risk levels. Every company must accept some risks to facilitate business and make their organization a place where employees and customers want to be.

For instance, technology companies favor more open offices with fewer physical security barriers. Compare entering a Silicon Valley tech space with trying to get into a defense contractor located in Virginia. You'll quickly notice how each approaches risks or perceived security threats differently.

An experienced security threat assessment team will go to lengths to understand the company's values and risk tolerance. Then, they'll build their security and risk mitigation framework inside those boundaries to fit corporate strategy and build the safest possible environments.

This approach also increases the security team's ability to win partners across departments. They're more likely to have the resources they need to implement security plans when viewed as an enabler rather than a roadblock to progress.

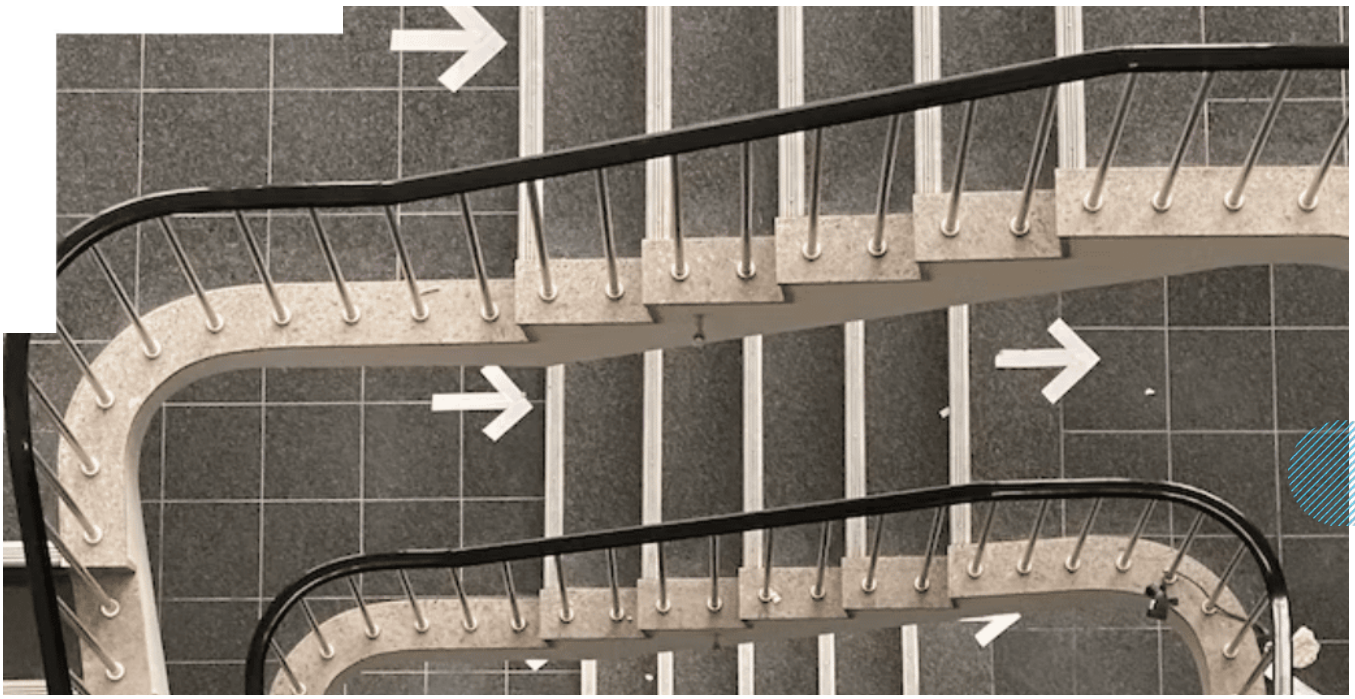
A strategic threat and risk assessment tells company leaders how to do something instead of why not to do it.

How to Build a Threat Assessment Template

A threat assessment template should be the first step once a security team cements its risk framework. The concept is simple; when everyone uses the same template, it leaves little room for misunderstanding. Everyone knows what information to provide, whether a new hire is doing their first assessment or the work is contracted out.

There are plenty of threat vulnerability assessment templates available online. A security team can likely get templates by asking vendors they hire or partners in the industry. However, the real work involves personalizing the template to fit individual organizations.

Thankfully, more options are now than ever that make creating and managing templates more efficient. While some companies still use pen and paper to note the location of broken locks and cameras, better choices are available.



Key Elements of a Threat and Risk Assessment

What are some of the critical elements of a cohesive threat assessment process? What should people be looking for to gauge and mitigate risk properly? Here are some things that every good threat assessment needs.

1. **Public Profile Examination** – A big part of assessing risk is looking at publicly available information about an individual or an organization. How can bad actors like criminals, competitors, or saboteurs use that information to gain access?
2. **Documented & Potential Threats** – Maintain an updated record in the threat assessment of actual threats and look at potential hazards that may be around the corner.
3. **The Physical Environment** – Physical environments impact risk. A high-profile celebrity is usually at greater risk of assault from an obsessed fan than a less well-known corporate executive. The same goes for differences in local security conditions in places like the United States versus Ukraine.
4. **Current Security Measures** – How do your current security measures address documented threats and potential issues yet to develop? Look at whether security postures must change based on the other elements listed.

These four elements are the baseline for a practical threat assessment. Each organization will likely vary in what they look at and how they implement threat assessment findings.

Investing in Threat Risk Assessment Software

The most innovative threat assessment tools use software and cutting-edge data collection to better gauge threats and security responses. Here's how security managers and their teams use the latest tools to assess and respond to threats.

Cloud-Based Threat Assessment Platforms

Security software empowers teams across locations and functions. For example, on a shared platform, a person of interest (POI) investigator can update a report informing a regional security manager on security incidents so they can assign protective resources faster.

The cloud means corporate security has access to active threat management processes built on a specific threat assessment model wherever they are. In addition, your data stays safe with built-in business continuity workflows.

Real-Time Data

One of the main problems with traditional threat assessment techniques is they only capture the threat at the time. However, conditions constantly change in a turbulent environment, making regular updates critical.

Now, no one has to wait for the analyst to update the assessment template with the latest threat of violence or when an earthquake happens near a manufacturing facility in China.

Instead, empowered team members can update cases, make comments, or provide feedback on analyst projections. As a result, the threat assessment becomes a living document that sits on a single database instead of pieces of information spread across different email inboxes.

Outside Data Feeds

One major advantage of security software is that it gives teams access to public information feeds that inform decisions. Whether it's tracking crime around colleges for a campus threat assessment or following social media threats in response to an executive's public statements, the latest security software provides more information in one place than ever before.

Feed all the relative information into one platform instead of paying multiple vendors and sifting through feeds manually. In addition, users can filter data based on what is needed at the time with access to public information relative to the overall threat assessment.

Cohesive Cases & Reports

People, particularly non-security stakeholders, are increasingly unlikely to read long security reports or assessments. Instead, they favor short, direct reports communicating events, data, and facts. One of the benefits of a threat assessment software platform is that it can quickly generate reports with just that. Security teams can choose to add insight, but they can also send out a Be On The Lookout (BOLO) report before the next annual shareholders meeting with a few mouse clicks.

The software allows security groups to scale much faster. On a cloud-based platform, users can generate threat assessments for locations, facilities, POI activity, events, and other intelligence requirements.

Clear Escalation Paths

Many organizations have detailed threat matrices that help security supervisors and directors understand the appropriate response in the face of any given threat. There will be, of course, exceptions to most rules, especially in unpredictable situations. However, a shared threat assessment on a software platform helps everyone better understand when and how to escalate any security threat.

After the Initial Security Threat Assessment

Most corporate security programs have processes that outline threat assessment protocols. However, what to do with the threat assessment after completion is usually a significant roadblock. Either the report quickly becomes outdated, or different departments generate additional reports because they can't find it or don't know it exists.

The latest threat assessment software changes how teams use the results to inform action. Threat assessments are living documents constantly updated according to current conditions and security postures. As a result, security teams can adjust faster to new threats and how they'll respond using scenario-based intelligence.

The audit trail of a digital threat assessment also facilitates after-action reviews (AAR), where companies can assess resourcing and how they respond to incidents or suggestions in the assessment. In addition, departments can identify security gaps by looking for trends based on how certain security measures lowered risk exposure in real dollar and life safety terms.

Software also offers new employees simulated threat assessment training that readies them for real-world experiences. For example, supervisors can task new investigators with creating cases, updating files, searching for social media keywords, and other components of a comprehensive threat assessment.

Asking for Outside Perspectives

People usually adapt to security threats around them. Someone's normal can feel very dangerous to someone unaccustomed to living in a high-risk environment. On corporate security teams, leaders must ensure their threat assessments aren't clouded by assumptions or acclimation.

Asking for outside help from threat assessment professionals is a terrific way to identify gaps or new ways of thinking. Working with experts in the threat assessment field often leads to new ideas on managing risks to a company, its assets, or its employees.

Effective teams call on experts for support with complex threat assessments or other unique situations. Whether you're creating a new program or want a refresh, some very experienced security providers will lend a hand.

When selecting outside support, find someone familiar with threat assessment software and the latest tools to empower the entire security team. They will work with you to establish best practices around using threat assessments and action plans for future growth.

The Value of Threat Assessment Beyond Security Teams

Evolving threats and more security risks mean more people are likely to rely on threat assessment tools and threat risk assessment software to guide companies forward. Gone are the days when the assessment was passed around between security managers and filed away. Now, the benefits of modern threat assessment techniques extend beyond physical security.

For example, legal and human resources teams can use shared security software platforms to take advantage of the audit trail they provide. Each case or report has a digital fingerprint from everyone who contributed to the report, which makes collaboration faster.

In addition, regional and enterprise incident management teams (IMT) can access shared platforms to assign tasks, establish a clear threat assessment process, and model future scenarios.

Tools for Strategic Reviews

Threat assessments are fantastic tools that help teams perform strategic reviews. Leaders regularly examine existing practices and resources as they look toward building security plans for tomorrow's threats. Detailed threat assessments highlight the effectiveness of a given program or point to holes that must be filled.

Years ago, most corporate security teams conducted strategic reviews by sending out surveys or spending thousands of dollars on airfare to bring groups to one location for meetings and discussions.

Now, however, that's no longer necessary. The modern threat assessment provides a timeline of events and actions taken throughout an incident. For example, suppose there was a security incident at a live concert. In that case, a security team can conduct a deep dive into the pre-event security checklist, assess any POI reports, how well the team involved local law enforcement, and other factors to understand what they may have done differently.

In addition to specific security incidents, an updated threat assessment is fantastic for spotting trends in data that indicate either an increase in physical or cyber security investments or a scaling back based on reduced threats.

Start Building Your Threat Assessment Training Program

The best corporate threat assessment programs involve a unified approach across teams that is consistent and adequately addresses risks to the company. In addition, security managers must have confidence that whoever is reporting, updating, or escalating threat assessment reports will follow protocols and, when necessary, make the right decision to protect people, assets, and reputation.

This is only possible with effective training. Employees and stakeholders need regular exercises to understand the threats facing the company and how to manage risks. When people know what to look for and how to respond, threat assessments make more sense.

In Ontic's 2022 Mid-Year Outlook State of Protective Intelligence Report, 98% of survey respondents said threat management training or behavioral threat assessment is important for their team to do their jobs successfully.

Here are some things to consider as you build your threat assessment program:

- Standardized checklists and protocols
- Involve threat management experts
- Use real-world scenarios
- Step-by-step threat assessment software demos
- Address various risks (business continuity interruptions, the threat of violence, etc.)

An effective threat assessment training program helps security teams design relevant training across corporate departments on:

- Threats of violence
- Natural disasters
- Long-term power interruptions
- Terrorist attacks
- Protests

Overall, formal threat assessment training clarifies roles and improves communication across teams. As a result, people know how to react. Doing the right thing is critical in high-risk situations or when a lot is at stake.

Managing the Expanding Threat Landscape

Corporate security teams face challenging security environments that will test their ability to protect their people and assets. Not only do managers have to respond to higher crime rates across many cities and countries, but they're also dealing with what seems like permanent changes to how we work.

For example, remote work is on the rise, and it's likely to stay in some form despite gradually returning to normal operations in a post-COVID world. How do security departments extend their threat prevention and risk mitigation to the home versus traditional school safety settings?

In addition to generation shifts in how and where we work, there is an increasing confluence between physical and cyber security threats. Even today, many cyber and physical security teams remain siloed. Unified responses are essential for organizations to respond to modern and future security breaches.

Building a comprehensive threat assessment program allows security teams to integrate with others to address cyber security concerns, legal threats, and reputational risks. The threat assessment then becomes the baseline for a company's response and helps them refine practices for the future.

Three Questions To Understand and Analyze Any Threat

No successful team strategizes to win without evaluating who they're up against. The same goes for security — a program has little chance of success without logically evaluating the risks or assessing the threat(s).

Understanding the Threat
The first foundational principle of an effective security program is understanding the threat, which should be the "center of gravity" for your security program. I will share the two most important questions one should ask before starting any security program.

1. What is the threat you're facing?
2. Why is the threat important?

Having completed countless after-action investigations on a range of attacks, I have learned a few lessons during those investigations. In essence, most successful operations carried out against a victim or entity usually boil down to three failure points:

1. Failure of threat intelligence;
2. A lack of tactical analysis of the threat; and
3. Vulnerabilities exploited in physical security operations by a range of threat actors.

For the last twenty years, I've had the pleasure of visiting with many billionaires and ultra-high net-worth families to discuss their security concerns and evaluate their risk profiles. To understand the mindset and their desire for security, I would always open with a few standard questions:

- Why do you think that you need security?
- What are the drivers for wanting a security program for you and your family?

Interestingly, the most common fear expressed was kidnapping, either of their children or significant other. Rarely did the individuals express concerns about themselves, even though many I chatted with were well-known and the public face of a successful company.

Invariably, at the end of my discussion, the Founder or CEO would ask for some quick advice, and my response has always been the same, "I truly don't know what you may need without first understanding the holistic threat directed against you, your family, and company."

I share this statement because a snap judgment without a comprehensive view of the threat landscape is never the path to take, even if the principal wants an immediate answer. A baseline threat assessment in Protective Intelligence is an opportunity to scope the threat landscape before committing or deploying resources.

Guided by Facts and Analysis

The second key ingredient is intelligence. Beyond facts, the analysis and application of those facts should be your guiding principle when designing a security program. For example, upon bringing the Protective Intelligence model to the private sector, while I knew that it would be a perfect fit, it required applying the methodology correctly. But, change management is often hard due to mindsets and legacy systems. Change happens when you apply data-informed intelligence to drive any program, which leads to our third question: How often does this threat occur?

For example, was the threat a one-time instance, or is there a pattern? Are there anomalies or deviations from your baseline? This is where intelligence comes in. The data defuses the emotion around the situation and allows a focus on the application of intelligence toward the resolution of the threat.

Technology tools help with various collection sources, curation of the singular instances into intelligence, and alerts to stay ahead of adverse incidents.

Key Takeaways To Understand and Analyze Any Threat

To best understand what you are guarding against and avoid a backward build of your program, you must first ask these three questions:

1. What is the threat you're facing?
2. Why is the threat important?
3. How often does this threat occur?

As you design your Protective Intelligence program, seek to understand the threat or threats in your environment. Figure out who dislikes you or those assets you are guarding. Trust me when I say this: You will find people, and sometimes even nation-state actors, looking to cause trouble. Leveraging intelligence and data to assess whether this is an anomaly or a pattern may require investment in technology, people, and processes to support scaling your protective efforts. Knowing proactively and building your Protective Intelligence program around it is always better.

Protective Intelligence and Surveillance Detection

By: Fred Burton

Protective Intelligence can be described as the process of gathering and assessing information about entities that may have the intention and capability of harming you and utilizing this information to protect your assets.

As more and more individuals and corporations have begun to realize that early preventative measures are preferable to emergency reactive ones, many organizations over the last decade or so have begun to adopt a more proactive approach toward security. And once you start down the positive path of proactive prevention, you're likely to reach some form or another of Protective Intelligence.

Protective Intelligence is the interesting juncture where you begin to expand outwards from direct physical protection and enter other realms like online presence, remote information collection, open-sourced information, communications, and surveillance detection.

A good way to visualize this idea is to think of reactive mitigation as your innermost circle of physical security. Around this initial circle, we extend a larger outer security circle of proactive prevention. Around that circle, we extend an even larger circle (one with an undetermined size) of Protective Intelligence.

From my experience, one important factor that needs to be improved in many Protective Intelligence contingencies is their field component – the connection between the cyber or open-sourced dimension and the physical reality on the ground. Without denigrating the importance of open-sourced or otherwise remotely obtained intelligence gathering and analysis, there is always a need for intelligence to also be gathered from the field.

It's not that remote intelligence collection isn't important. On the contrary – that's where you want to start. But this first resort shouldn't be your last and only one. As I had detailed in an earlier article, hostile planners use open-sourced intelligence in their Hostile Planning Process. Still, they don't stop there – they follow it up with field intelligence, i.e., surveillance. So if hostile entities know better than to only rely on open-sourced intelligence, why would a Protective Intelligence contingency not do at least as much?

What is Intelligence?

In a well-written article by Kristin Lenardson and Charles Randolph (two very experienced and highly regarded experts in Protective Intelligence), an important distinction is made between intelligence and information. Intelligence, the article explains, is information that is contextualized for your needs. "You discern what information is actually important to your principal and the detail; this turns the information into intelligence." The article also emphasizes the need to diversify your sources of information – to not depend on any single source by itself.

The points I'm trying to make here are that a) when it comes to physical assets, a very important source of information is the actual situation in the field, and b) your ability to discern between what is or isn't relevant or accurate depends on a certain amount of field verification.

It ultimately comes down to what questions you want answered. If you want to find out what people are saying about you online or who's been researching, coordinating, and communicating about you lately, then cyber or open-sourced avenues might very well provide you with the answers you're looking for. But if you also want to find out whether anyone has been physically surveilling your corporate headquarters, the residences of your executives, their routes to and from work, your special events, or any other important asset (remote databases, employee vehicles, etc.), then you're going to need another – more physical – avenue to answer these types of questions.

The field component of your Protective Intelligence effort (usually SD) can provide two very important functions:

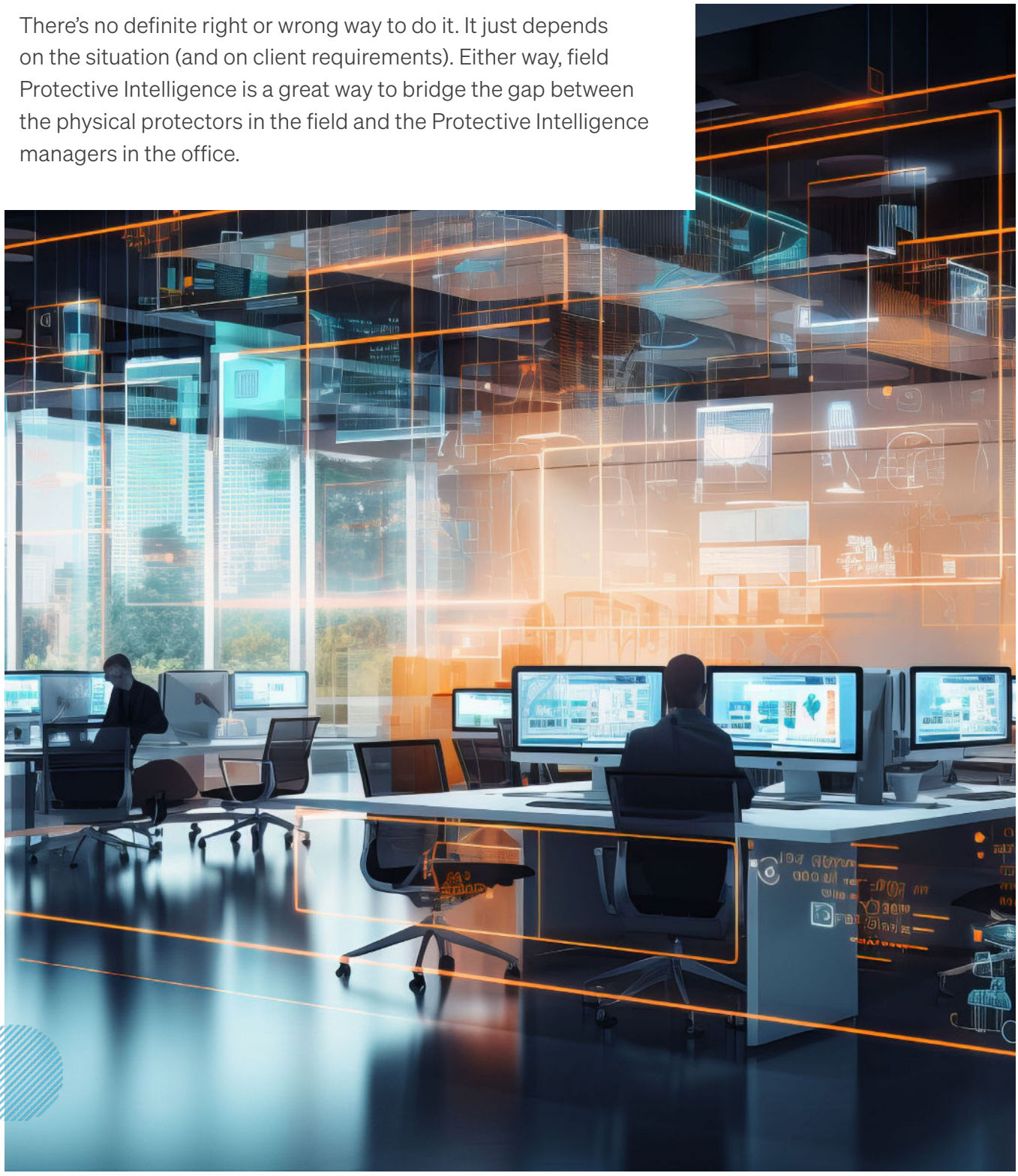
1. It can collect vital, accurate information about real-world events, situations, and activities in real-time, and do so in conjunction with a professional analysis of what it means (oftentimes on the spot). No open or remote source can currently provide this.
2. It can verify the accuracy of your open-sourced intelligence using physical data – in real-time. Open sources can be very important, but until they are put to the test – until you have actual evidence from the field – they essentially provide you with unsubstantiated claims. If you never see how open-sourced intelligence does or doesn't physically manifest itself in the field, how will you know if it's good, verifiable intelligence?

I have lost count of how many hundreds of private and public sector open-sourced or otherwise remotely collected intelligence reports I or my clients have received over the years. These reports can be very useful in their own way. But in most of the cases where they're not also accompanied with, or supplemented by, a field intelligence component (usually SD), they provide not much more than vague and general BOLO alerts and security advisories that don't always leave you with much to go on. If all you're looking for is to revise some theoretical threat matrix to present to a security committee, then that's fine. But if you're interested in proactively preventing harm to your physical assets, you'd be well advised to incorporate a field component into your Protective Intelligence program.

The main value of surveillance detection is that it straddles, and therefore bridges, the two realms of security and intelligence, which is why I view it as a form of Field Protective Intelligence.

Interestingly enough, SD can be employed by a physical protection program that sends operators out to take positions around it (from the inside and out), or it can be employed by a Protective Intelligence program that sends operators to the field to be closer to the action (from the outside, in). I've done it both ways for corporate clients; in some cases, reporting to the physical protection team, and in others, reporting to the Protective Intelligence Center.

There's no definite right or wrong way to do it. It just depends on the situation (and on client requirements). Either way, field Protective Intelligence is a great way to bridge the gap between the physical protectors in the field and the Protective Intelligence managers in the office.



Protective Intelligence While Working Overseas

By: Fred Burton

It's no secret that the world is a dangerous place. Organizations with international operations and executives traveling abroad face various risks, from terror to weather to inadequate law enforcement resources. This is also a hard lesson I learned a long time ago while employed as a special agent with the Diplomatic Security Service looking into attacks on diplomats and businesspeople around the globe.

One of the first cases I looked into was the murder of a Black & Decker employee in Lyon, France. The employee was gunned down at his doorstep by a terrorist organization in April 1986. The LA Times reported that the murder was committed in response to the U.S. raid on Libya. Later, in 1989, Alfred Herrhausen, a German banker and the chairman of Deutsche Bank was killed in a brilliant and sophisticated bombing operation by the Red Army Faction in Bad Homburg, Germany (this is described in detail within the National Institute of Justice's report on Terrorists Tactics and Security Practices). We would study the Herrhausen attack for years as an example of the sophisticated targeting of a prominent business person.

Of course, executives aren't the only individuals targeted for assassination. In September 2020, Afghan Vice President Abdul Rashid Dostum survived an assassination attempt that targeted his motorcade in Kabul. Global News reported that the attack killed 10 and wounded over 30, including many bodyguards.

Consequences of Global Threats

Foreign policy actions have consequences, such as the targeted assassinations described above. In some cases, those actions are directed towards Westerners who have become softer targets than their government counterparts in the country. Why? As U.S. Government facilities and embassies have been hardened with physical security measures, the threat has been pushed into the private sector, where security measures are typically much less stringent.

Other less obvious factors come into play that are worthy of discussion. For example, significant risks can be involved in meetings with foreign government officials and executives. This is heightened in places that face a deteriorating security situation or those that would draw the attention of nation-state intelligence services.

Even if your protectee is not being directly targeted, there is a significant risk of being in the wrong place at the wrong time or caught in the crossfire if someone nearby is targeted.

Let's be frank: a Western CEO or senior executive who meets with a foreign leader will cause the intelligence services of many countries to take notice, likely putting that executive into the crosshairs of several intelligence organizations. The same is likely true of meetings with many pivotal business leaders, especially those within industries critical to national security or economic competitiveness. Nation-state intelligence services exist to steal secrets, competitive intelligence, and any other nuggets that can be collected for various foreign policy, financial, and critical intelligence purposes.

Best Practices for Mitigating Threats Overseas

So, how do you mitigate these concerns? Here are a few best practices and lessons learned to consider:

Evaluate Executive's International Meetings and Attendee List

First, ensure you have access to the executive's international schedule to determine where the meetings will occur and who will attend. Consider what threats might be "dragged" into the meeting. For example, if you are meeting with a senior Mexican official or Russian oligarch, what threats could there be on that person's life that you can anticipate? Are drug cartels or organized criminal groups likely interested in or involved with any attendees? Are foreign intelligence services likely to be interested in the meeting? All questions are on the table.

Location–Specific Risks

Before departure, a threat assessment needs to be conducted to determine the likely risks for each location on the itinerary — these should include health, cyber, and intelligence risks such as hotel listening devices or drivers working in collusion with nation-state actors. In some countries, these problems are a given (e.g., China, Iran, and Russia) and are unavoidable.

Advanced Notification to Overseas Partners

As part of the travel advance process, protection personnel should also contact OSAC and the respective U.S. Embassy Regional Security Officer for notification. Where possible, you should also seek reliable local security advice about the best places to stay and for reputable local support, such as drivers, good hospitals, and any other local concerns that wouldn't be immediately apparent or that could arise specific to your executive's itinerary.

Use of Clean Devices for Travel

Consider using "burner" phones and clean laptops for executive travel. This is often easier said than done, as we know, but the issue should be raised, especially for high-risk travel or companies facing a high risk of corporate espionage. Once back in the home office, your IT team should carefully scrub those travel devices to determine if any malicious activity occurred and ensure nothing was left behind on the devices by a nation-state actor.

Consistent Monitoring of all Devices

For the actual meetings, I have always found it best for the executive protection officer to secure the executive's laptop and cell phone to reduce the chances of those electronic devices being compromised. Once those devices are left behind, let's say in an adjacent room, you should assume that they have been compromised.

While it isn't always possible to entirely avoid all risks, executive protection professionals should carefully consider these threats before facing them in real-time. Discussing these scenarios ensures that all parties know the potential problems and consequences. Understanding the threat profile helps all parties make the best decisions to keep executives and the company's information safe.

How To Recruit and Select a Protective Intelligence Analyst

By: Fred Burton

There are many considerations to keep in mind when looking to hire a Protective Intelligence analyst to support your corporate security operations. In our experience, the security industry (excluding infosec) generally offers a hiring manager limited standards to judge a candidate's competence. This is doubly true for managers seeking to hire a Protective Intelligence analyst. There are no analyst certifications — and it's not clear that any certification or university program alone would be sufficient proof of one's competence.

This leaves hiring managers facing a massive challenge in defining what makes a candidate qualified to be a Protective Intelligence analyst, and finding quality analyst candidates is a challenging task. It's these topics that we'll explore in detail below and offer solutions that our team of corporate security leaders have come to rely on over the years.

What Characteristics Should You Look For In a Protective Intelligence Analyst Candidate?
There are two ways to answer this question. There's the book answer, and then there's the pragmatic answer.

Let's start with the book answer by considering a work that has already touched on this. In "Intelligence Research and Analysis" by Jerome Clauser, he makes the following observation:

> *"Ask any authority to identify those human traits that are absolutely essential for anyone proposing to carry out research and four traits are mentioned invariably: reasoning ability, accuracy, intellectual honesty, and open-mindedness."*

He then goes on to mention the following secondary characteristics:

- Skepticism
- Detachment
- Patience, Diligence, and Perseverance
- Imagination

That's the books answer. And it would be no easy task to identify these characteristics during a phased selection process.

Here's the pragmatic answer that is far from perfect but easier to apply in your work.

What I'm most concerned with when evaluating an analyst candidate is that they work hard, write well, have a positive and curious attitude, and have an interest in working with "things" (as opposed to people). That's it. I can work with anyone who fits these four criteria, and anyone who fits these criteria can be trained to reach Clauser's ideal.

A quick note on what characteristic to avoid at all costs: arrogance. Protective Intelligence work is not "sexy". If you hire an analyst who is unwilling to get their hands dirty with work that could be described as mundane, then they won't be a good fit. Lots of security work is dry, and not what you see in the movies. So, we need support from people that aren't "above" doing the work. We need team players in the trenches with us, not primadonnas.

What Are The Core Competencies of a Protective Intelligence Analyst?
I could write a book about this topic alone, but for brevity's sake, this section will be as high level as possible to give you general guidance rather than a prescription.

1. Communication is the most important competency for an analyst. In this context, communication means many things: written, verbal, presentation ability, and the ability to package information in a form most appropriate for a given consumer.
2. Research ability is critical. Analysts need to be highly competent at finding information. This means knowing what sources to visit and how to drill down to the information they need.
3. Moderate technology savviness (at a minimum) is increasingly important. Analysts need to know how to make technology work for them. The availability of information is enough to overwhelm anyone, so analysts need to know how to use automated tools that collect the information most relevant to their mission.
4. The analyst must understand the perspective of "the man/woman on the ground" – empathy. This is not a new idea. When you have analysts in the GSOC who have worked a security detail, tried conducting surveillance (even in training), have responded to a disaster, etc. — this is what separates good analysts from great analysts because they intuitively know what information the person on the ground needs to accomplish the mission.

Where Do You Find Intelligence Analyst Candidates?
First, consider the possibility of a future Protective Intelligence analyst sitting right under your nose. It's common for those working in "field" security roles to transition into analyst roles. Consider this: they already have all of the knowledge of a field operator, which can be used to inform their future work as an analyst. This is a great option if you're willing to personally train or pay for additional training for this type of person interested in transitioning. I recommend strongly considering this, especially if you already know this person to be reliable, hardworking, and a decent writer from your previous experience with them.

Second, you can find them in universities and related internship programs. A great number of universities in the US use online platforms to connect their students with internship/job opportunities. I encourage you to contact your local universities to learn more about these types of opportunities. Administrators will be more than willing to help and direct you through their process. A more effective option might be networking with individual professors who teach courses containing students who fit the analyst profile.

Generally, I think those who have an interest in international relations/political science, criminal justice, or psychology tend to transfer their interests well to Protective Intelligence. Of course, no college program prepares one for Protective Intelligence work.

Instead, think about the rigors of the programs and how those transfer over to analyst-type work. In the above-mentioned disciplines, especially international relations, there are lots of reading and writing about "dry" material, and the student has to learn about diverse events, systems, and interactions among countries — all of which relate to the work of an analyst.

Lastly, an additional source to consider for finding analyst candidates should be internship programs with law enforcement agencies (e.g., local PD analysts) or researchers with think tanks.

How Do You Select The Right Candidate?
I like to think about candidate selection in three phases: information gathering, testing, and interviewing.

In the information-gathering phase, you are simply vetting the information provided by the candidate. This is likely an application of sorts, a resume, a letter of recommendation, and a writing sample.

What are you looking for during this information-gathering phase? I would be interested in their academic background/performance, work history (does anything here indicate focus, stability, grit, etc.?), projects they're proud of, and their ability to put together a resume. For example, if they present you an intelligence product in a similar way to their resume, would you read it?

When it comes to testing candidates to guarantee a minimal level of competence, there are a number of routes. A common practice is for hiring managers to give a candidate a test demonstrating their ability to research an issue and present it in the form of a written product. This could be as simple as relevant news media relating to a CEO's hometown or an in-depth project to create a trip briefing or investigate a fictitious person/company. A deliverable based on this type of test should give a hiring manager insight into how the candidate thinks and how competent they are at researching and presenting information.

As a side note, I haven't seen much of this yet, but I can see investigative teams and security teams in the future using other tests to identify the best candidates. For example, if you know that your most successful analysts have specific traits or characteristics, why would you not screen for people who fit this success profile? Plenty of evidence supports the consideration of these types of tests in the future.

Finally, there's the interview phase. I won't tell you how to run an interview, but I will share what I've found helpful. Interviews are a great chance to learn about the candidate's thought process when they conducted your initial test (What did they struggle with? How did they adapt?). Additionally, the questions I've found to be most revealing are those about professional development (What books are they reading? What investigative or analytical books/courses have they found useful? Have they read any books from ATAP's reading list or the author Michael Bazzell?). These questions, among others, demonstrate the candidate's thought process, approach to learning, and more, will be very informative.

Assessing An Executive's Digital Footprint

A key element involved in understanding the threats, vulnerabilities, and associated risks to an executive is the assessment of their digital footprint. The ultimate goal is to surface what information is available online for a savvy adversary to exploit. This information could include details about the executive's travel movements, satellite imagery of their home(s) on Google, or even online material of one of their family members or associates that could embarrass the executive.

Getting Started

It can be overwhelming to know where to start when assessing what is available information on an executive. One way to think about assessing their digital footprint is to categorize findings in one of three areas:

- **Attack Cycle Planning** — There are critical details that an adversary can use to conduct an attack which point to the theme of "time and place predictable," giving an adversary advanced information to use in their attack cycle planning. (e.g., an executive's assistant posting publicly about the executive's schedule)
- **Low Urgency Information** — While not to be overlooked, there are less-critical details about an executive, such as their phone number, email, or family office address being leaked publicly that could still facilitate an adversary's planning phases of an attack.
- **Reputational Information** — Reputational damage is extremely difficult to repair. A frequent example of this category includes a family member's behavior on social media or an executive's participation in online communities.

Sourcing and Research

Limitless sources can be used to conduct this type of assessment — this is certainly not an exhaustive list. Here are some examples of the types of sources that could be included:

- **Data Brokers** — Credentialed and non-credentialed data brokers should be considered, as nothing prevents an adversary from accessing non-credentialed sources. (e.g. BeenVerified)
- **Social Media** — It's critical to know what social media profiles associated with an executive (including family members and associates) are online and whether they are being actively used. It's also necessary to know how the content of those social profiles can impact the executive's safety and reputation (e.g., "time and place predictability").
- **Business Related Documentation** — Public business registrations or licensing documents that reveal sensitive information such as addresses, associates, contact information, and more should also be considered.
- **Political Contributions** — Many political contributions are made public via online sources.
- News Media — It's important to stay on top of any adverse or sensitive information that can be discovered via online and print media.
- **Asset Related** — Sensitive information that can be discovered via public sources related to asset ownership should be identified (e.g., property deeds, vehicle records, etc.).

Guiding Principles

An important principle to use as a guide when conducting this type of assessment is: How do the people around the executive influence the executive's safety and reputation? This is sometimes called "threat by proxy" or "targeting by proxy."

First, if those around the executive are the target of threats, that puts the executive at risk because of their proximity and association with the targeted person. Second, even if the executive at the center of the assessment is diligent and does everything to prevent sensitive information from being easily accessible to an adversary, safety is not guaranteed. Individuals surrounding the executive could have poor safety and security practices, which an adversary can exploit to harm the executive.

Steps to Mitigate Risk

Thinking both short term — to address immediate issues facing the executive — and long term — identifying proactive steps to fix the processes in place that likely create vulnerabilities — are a valuable combination of activities. Our recommendations include:

1. Reduce online activity and limit information that potential adversaries can exploit.
2. Educate close associates about how to safely use social media, using social media threat intelligence and digital privacy tools to prevent the leaking of sensitive information, including contact information (e.g., email forwarding, burner phone numbers, etc.).
3. Remove old social media accounts no longer in use, as well as business entities, trusts, etc., to protect personal information relating to assets.

SECTION III

Protective Intelligence Tools and Technology

Digital Transformation and The Evolution of Corporate Security

Protective Intelligence has always been focused on the future — seeking to prevent risk events from impacting the organization. With a focus on proactive synchronization across channels and landscapes, security teams bring a preemptive approach to managing threats. Tactically speaking, how do we take that same type of forward-thinking approach and apply it to corporate security teams? The backbone of this approach is digital transformation.

In thinking about digital transformation and the role of technology for security teams, there are three evolving areas:

- **Proactive Threat Assessments (including tactics used)**
- **Digitized Security Controls and the Internet of Things (IoT)**
- **Corporate Security Team Competencies**

The combination of these three areas sets the course for digital transformation and the evolution of corporate security teams.

Proactive Threat Assessments
Over the last year, there have been countless digital attacks against private organizations' assets in the news and many more that went unreported. These attacks take many forms and cross the cyber and physical realms.

- First, there are events such as the SANS Institute hack, where an adversary gains access to an organization's data by phishing a single employee and then leverages their account to steal sensitive information or even hold it for ransom.
- Second, and perhaps most disturbing, insiders within an organization are using digital resources/assets of the organization in an unauthorized manner that harms the organization's reputation and share value, similar to this past insider threat incident at Tesla.
- Finally, the more routine aspects of accounts are being compromised because employees need to follow elementary security practices (e.g., post-it notes with passwords and not exercising skepticism).

These are some of the ways that digital transformation has created new threats. However, it has also led adversaries to adopt new approaches and methods for targeting organizations.

One primary tactic adversaries adopt is endless and organized social engineering attacks against organizations. Account takeover is one of the most common and one of the most damaging threats modern organizations face.

This can lead to endless immediate-term issues, such as data being encrypted/held ransom or the company being blackmailed into paying a fee to prevent public humiliation. The long-term consequences are loss of consumer trust and a declining stock price.

> ***TIP: Simple but effective controls for preventing these types of incidents include employee security awareness training, implementation of MFA (multi-factor authentication), and more.***

A second approach by threat actors is intellectual property theft — especially that which is facilitated by foreign governments. Over recent years, this has garnered significant media attention. U.S. Government sources have written endlessly about how foreign governments use varied methods to spy on and steal from private organizations. These methods range from systematic, financed hacks facilitated by foreign governments that take place over years, with the goal of stealing proprietary information. It also includes foreign government's initiatives to plant government agents in privileged positions, such as the DOJ's case against a former Stanford University researcher from early 2021.

> ***TIP: Preventing intellectual property theft is no easy task. However, the implementation of an insider threat program that vets potential new hires and puts safeguards in place to alert security teams of unusual activity (e.g. using an external hard drive to save company files) can provide a layer of protection.***

Digitized Security Controls and the Internet of Things (IoT)

Yes, digital transformation has widened every organization's attack surface — but it's also empowered security programs to a point where they can accomplish more than their predecessors ever dreamed.

One of the key drivers for this is the converging of networks driven by connected devices and the IoT. Security systems of all types (physical and information-based) are leveraging information like anomaly detection, running process rules ("if this, then that"), and triggering alerts.

Individual hardware devices like access control, cameras, and location detectors are increasingly connected to create an expansive network for information to move across. This has become a powerful force for security teams as that information is quickly turned into intelligence, triggering process rule-based protective measures.

For example, if a pre-incident indicator is detected (e.g., the badge of a terminated employee is used), then take this action (e.g., do not allow entry, flag section of video footage, and send an alert to the security manager across devices all within seconds). While somewhat rudimentary, it serves as an important foundation for managing an expansive threat landscape and putting automation in place to thwart potential incidents.

Digital transformation in security continues as smart security systems work to develop a "pattern of life analysis" for users/employees/others. This means that when something out of the norm occurs (e.g., a user uses an unusual amount of bandwidth or logs in from an unusual location), then security resources are alerted to investigate the anomaly. This type of technology is being applied in many information security contexts and in the near future, will likely be applied in more physical security contexts such as access control systems, and more.

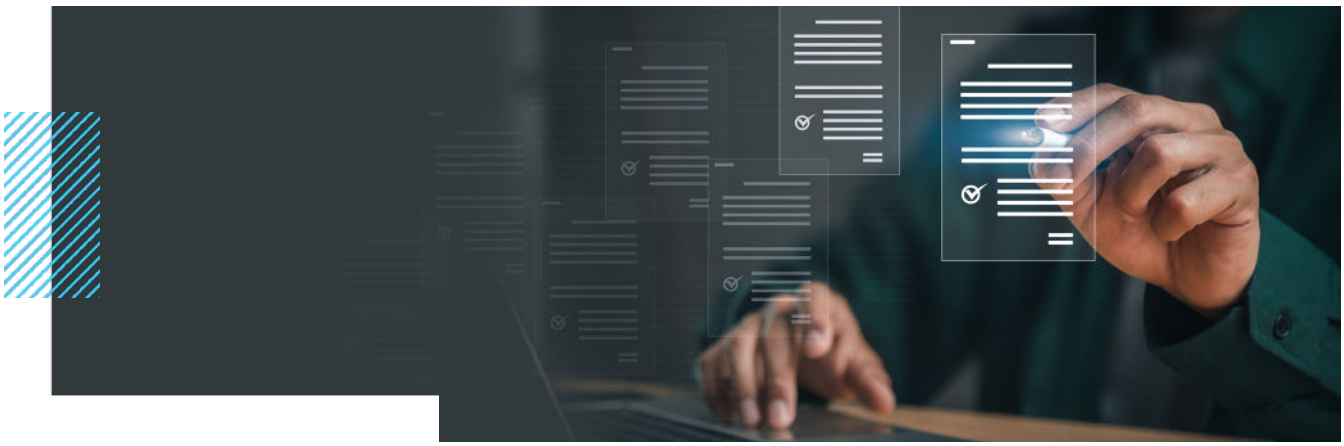
Corporate Security Team Competencies

Even with 20+ years' experience in corporate security and having attended every workshop held by ASIS — this may not thoroughly prepare you to brief an executive on corporate security strategy. Increasingly, information-based issues are top of mind for executives, and every security team is responsible for being able to speak to these topics (at least at a high level) and then employ the right team to execute and protect the organization's assets.

Be prepared for digital transformation in your organization by embracing the humility of our security prowess and the convergence of cyber and physical security efforts:

- Embrace continual learning. Dedicate time to learning about the common and high-impact digital challenges facing organizations and how our peers are addressing them. ISC2 and SANS Institute offer many resources and host events to help in this area.
- Have an up-to-date rolodex. Befriend true, reliable experts that you can consult on niche topics when you are outside of your "wheelhouse." No one can be an expert on all security topics, so borrow the brainpower and input of your peers.
- Remember that technology requires humans to execute. No matter how awesome your security technology is, the mission can't be accomplished without engaged security practitioners behind the wheel. Dedicate time to developing talent and taking care of the troops.

Led by digital transformation efforts, organizations continue to evolve. New, connected devices and new, connected threats call for an evolution in the competencies required by corporate security teams. How we adapt to the changing landscape of threats will define protection and the next generation of corporate security professionals.



Six Things to Consider When Buying a Case Management Solution

Despite the fact that leaders in physical security, cybersecurity, IT, human resources, and legal and compliance all deal with threats and business risks, each department often has a unique method and tool for documenting and managing incidents. These organizational divisions across departments isolate threat intelligence and negatively affect business continuity. In a recent study, 50% of C-level executives said that if teams shared and accessed the same intelligence in a single platform, at least 51% of threats that impacted business continuity and resulted in harm or death might have been prevented.

A security team's operation has long included gathering and collecting threat data and handling events, investigations, research, and cases. In the past, solutions developed to reduce manual labor in these sectors have not been designed in an open, flexible, or contemporary manner to enable teams to change with the times. The need for modern and adaptable case management technology has never been greater than it is now.

The Problem with Most Case Management Solutions on the Market Today

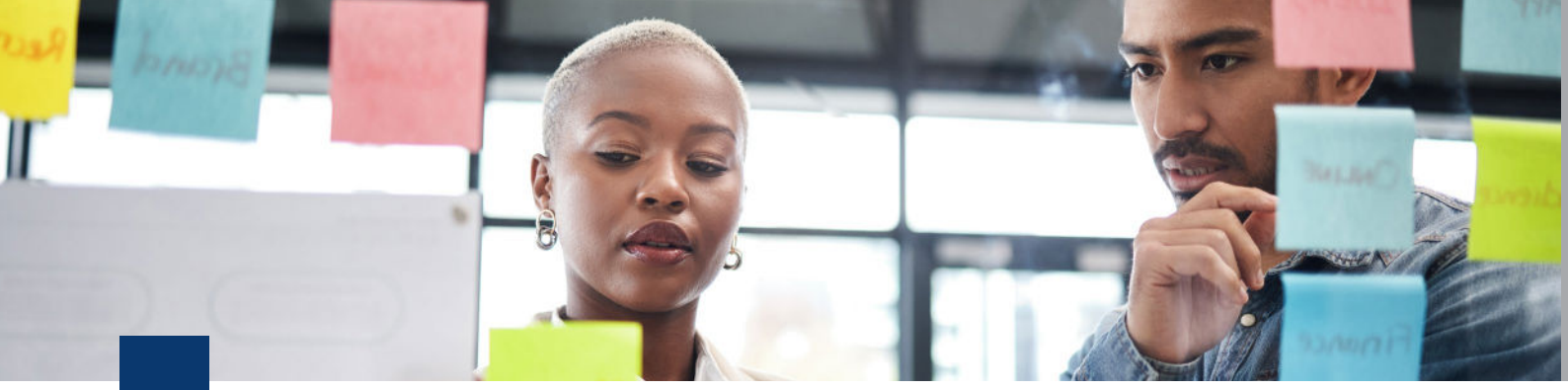
Reporting and managing incidents and events in spreadsheets and documents might result in crucial information slipping through the cracks in this heightened threat landscape. Although the security sector has started to use technology, security teams typically find it difficult to adapt because these single-use solutions are frequently inflexible and outdated. The more layers of point solutions teams add, the more they face the complex task of trying to piece together a holistic picture of risk intelligence.

Aside from being complex and hard to use, most solutions on the market currently:

- Are heavily incident-focused with little ongoing monitoring
- Lack external data connections and system integrations resulting in the manual entry of data
- Lack customization and reporting capabilities with limited metrics that require manual exporting
- Lack advanced capabilities for situational awareness
- Focus on reacting to insider threat incidents versus proactive investigations
- Have limited collaboration and communication across departments
- Come with high maintenance charges, lack of training, and a dedicated support staff
- Have cumbersome workflows with limited flexibility

Six Things You Should Be Looking for in Your Case Management Solution

Implementing centralized investigation and case management software helps modernize security teams' operations. It's essential to have a comprehensive case management system if you want to actively reduce risks in your business. With the right systems in place, security teams can effectively implement the appropriate response to incidents, collaborate on cases across teams, and minimize organizational risk.



If you're looking for your case management tool, here are the top 6 things you should consider:

All-in-one flexible and customized experience
It's imperative for the software to offer the flexibility to configure and manage the complete incident, investigation, and case management lifecycle. Every aspect of the investigation workflow and output should be self-service and customizable to ensure consistent documentation of data collection.

Meaningful insights with dynamic metrics & reporting
Filter through the noise and track what matters with resource metrics, timelines, and cost details for consistent reporting and critical findings to build trust with leadership and reduce business disruption. Configurable, platform-curated dashboards and reports are key for investigation results, case statuses, and reliable risk mitigation.

Always on integrated research and intelligence
Always on, fully integrated suite of research tools will provide the most complete set of real-time and historical public records data. An open platform integrates with systems for continuous connections to data sources and integrated tools for automated updates of new information or activities.

A fully connected, centralized solution
The right tool should have a collaboration-first experience with one centralized place for inter-team, cross-department visibility and coordinated action. With connected processes and workflows, teams can maximize efficiency and be more effective while maintaining a full picture of their threat landscape.

Real-time threat detection capabilities
Detecting threats in real-time surfaces key signals for corporate security teams rather than relying on analysts to enter events or sensor data. Gaining situational awareness will save time and speed up the investigation process by connecting relevant information faster.

Advanced threat assessments
Leveraging custom threat assessment methodologies within the software will continuously and automatically scan for information to uncover critical signals that allow teams to take early action and minimize risk. The signals can trigger customized workflows, so teams know the right action that needs to be taken.

Mobile Applications are the New Norm in Protective Intelligence

By: Fred Burton

I'm a big believer in understanding how we got here. Due to Protective Intelligence failures, our efforts to identify surveillance were born out of necessity. Our mission was pretty straightforward in the early days of surveillance detection. Hunt for surveillance. Watch for the watchers. Look for people planning inappropriate contact with a high-profile person or planning an attack.

In principle, it sounds simple, but tough to do in reality.

We operated in the shadows, in cars, bicycles, and on foot, separate from the traditional protection team. We were a poorly dressed crew and did not stand out from the crowd. But, we became very good watchers. I learned that you could sit for hours on a park bench or bus stop without anyone noticing you, and to this day, I think about that every time I pass a bus stop.

The technology we used was from the 1970's. Binoculars, Polaroid cameras, big Sony recording devices with VHS tapes, Motorola radios, and pagers. Our intelligence feeds were transmitted via pagers or shared over a radio, which was always hard to hide. I can still see a protection officer we were training on a bench in New York City talking into his rolled-up New York Times, with his radio antenna sticking out. The video of the officer talking into his paper was priceless and far from discreet.

Our teams worked with lots of paper, handwritten notes, or typed BOLOs stuck in shirt pockets, Banana Republic vests, and placed above sun visors of non-descript cars. At times, all we had to go on was a grainy black-and-white surveillance photograph of a person of interest (POI). Many were thumb-tacked on a wall beside my wooden desk, above the Rolodex and 3×5 cards, which was my database.

In the field, Protective Intelligence information was stored in command post hotel rooms and handwritten into a surveillance log. After the detail, incidents were data-based for future use, as time permitted. Our ability to vet a threat on the street was challenged, to say the least, because technology and smartphones were still on the horizon.

That is no longer the case. We have crossed a new frontier into threat detection with mobile applications. Mobile apps are the new norm.

On a practical level, why is a mobile ability so important? Information is the lifeblood of any protective mission, and threats are mobile. POIs move with the protected person, and fixated persons stalk their prey. POIs lurk, travel, drive by houses, visit offices, and show up in unexpected places. Time and time again, I've seen all these unhealthy actions occur. For the officer on the street, real-time facts and data matter. Pictures, videos, names, license plates, vehicle descriptions, and past incidents are required to do the job right.

A mobile app enables the officer to rapidly identify persons or vehicles with proximity risks.

Here are a couple of examples:

- A moving protection officer is not only keeping an eye on the executive but also watching for surveillance. It's also important to expand surveillance detection efforts near departure points. Having Protective Intelligence data at your fingertips enhances protection and provides a more secure environment for the executive or VIP.
- For efficiency's sake, security officers at a residence or on patrol at the main office should be able to research and catalog suspicious incidents, vehicles, and persons, because the same person can show up at different locations over time and distance.

Mobile apps should be part of every officer's gear like flashlights and radios. What I would have given for that capability and technology in 1986.

SECTION IV

Practical Application of Protective Intelligence in the Business World

The Enemy of My Enemy is My Friend: The Unification of the CSO And CISO

By: Tom Kopecky

Whether you are fighting anonymous digital adversaries or those operating in the flesh, it's fair to say that insider threats rank high on the list of public enemies in our security landscape. One of our advisors once said cyber teams use bits to protect bits, while physical security teams use bits to protect atoms. This is mostly true, although a lot of bodies are still required to protect physical infrastructure. For those of you about to gloss over at this point, hang with us, as I promise this is germane to the physical security intelligence practitioner.

The differences in the application of tradecraft by both cyber and physical teams are enormous. If you were to research the history of insider threats and related risk mitigation techniques, one would assume that insider threats are strictly a cyber problem that can only be solved by cybersecurity teams using their dedicated strategies and tools. After all, cyber seems to be well regarded as a safe and necessary investment, and it requires less scrutiny to obtain a realistic operating budget. There are about 1 million cybersecurity workers in the US alone, with approximately 700K positions yet to be filled. According to the Cyber Research Databank, there are over 3500 cybersecurity vendors globally.

In retrospect, physical security teams are often considered cumbersome, slow-moving, and highly reactive cost centers. They are not typically recognized as invaluable C-Suite resources who are instrumental to the overall business success of the enterprise. Cyber and physical security teams remain extremely siloed by nature, and who can blame them? They define risk differently and view the threat landscape through a completely different lens. The teams also speak a different language and mitigate threats in an entirely different way.

Many people continue to assume that the insider threat topic has been thoroughly vetted & defined and that a consensus has been reached regarding the best solutions for the problem. As you dig deeper and seek feedback from security professionals, it becomes clear that the interpretation of insider threat varies across security teams, and depending on who you as, mitigation strategies also vary greatly.

How do we unify the approach?

In all my years of conducting physical threat and vulnerability risk assessments, I am still waiting to see a fully unified cyber and physical security team. While the general perception continues to reinforce the rumor that cyber owns insider risk mitigation, we are seeing an interesting evolution occur right before our eyes, where CSOs and their supporting intelligence teams are not only joining in but, in some cases, leading the fight against insider threats.

How did this occur? First, we need to remember that when protecting a business from an inside threat, we aren't just dealing with digital assets, networks, servers, and firewalls. We have much more to protect, including vast amounts of physical infrastructure, including decentralized workforces, workplaces, intellectual property, supply chain, and all of their supporting cast members. To protect this vast network of physical assets, we need to ensure that we are looking in the right places for elevated risk. This involves monitoring access points and extended vulnerabilities that are created by humans – on-site and remote employees, vendors, contractors, and even those that are in the circle of influence of our customers. Much of the additional context can only be provided by monitoring and detecting three-dimensional human behavior in action.

We previously addressed how a cyber attack starts as an exploited physical vulnerability, and physical attacks are rooted in cyber vulnerabilities. Defending against an insider threat is much more than simply waiting for an alert from a Security Information Event Management (SIEM) platform. Although those systems will continue to remain critically necessary, many insider threat issues are detected because an employee or contractor circumvented physical infrastructure in the planning stages prior to a malicious act. That is why we need to use comprehensive intelligence monitoring techniques to help recognize threats well before they become a critical situation – because, at the root of this, a human somewhere is part of the planning and attack cycle.

To fight this battle effectively, we need both cyber and physical security teams to join forces to work together and agree on the most appropriate strategy for their organization. Remember – the majority of the required data, tools, and security leaders already exist in your company today. So we must ask ourselves:

> *Why is widespread collaboration between CSOs and CISOs not yet evolving on a broader scale – especially when we know that many insider threats are initially detected via physical security monitoring as well? And what does collaboration actually look like in real life?*

When analyzing many of the more notable incidents that impact supply chain, workplace security, and other critical infrastructure, I've noted that the insider threats that we deal with most are hybrid meaning that are initially detected as a digital signal or alert via a cyber monitoring system, yet have a significant nexus to physical infrastructure. Due to the nature in which the threats are planned for and carried out, many have physical risk indicators, which makes them detectable by systems that recognize human threat actor behavior.

This is why a proper physical threat-hunting program must complement and interface with your digital threat-hunting operations. Cyber threat hunting is key, yet it alone will not allow your teams to understand the bigger picture of the risk landscape, nor take the most appropriate action.

So, with the increased frequency of these types of insider threat incidents – the question remains:

Why is this collaboration of the CSO & CISO not yet evolving on a much broader scale?

We often notice that while cyber and physical teams have vastly different tactical objectives, their strategic goals remain the same, which is to reduce risk and liability to the company, its assets, and, of course, its people. For more insight on this question, Josh Massey, Department Manager at MITRE, provides his point of view.

> *The malicious actor does not think in terms of cyber versus physical, so why should security defenders? Rather, a motivated and malicious actor will follow the path of least resistance toward the desired target. This means a 'hard' physical target naturally funnels the adversary to the 'soft'' cyber target (or vice versa). In essence, 'my success is your demise'. Unfortunately, siloed security practices such as this lead to a zero-sum game where one can still claim success despite others' failure. However, a more collective approach would view the problem as we either win together or lose together. At MITRE, we've structured our insider threat program to eliminate the artificial, functional turf wars of security silos in favor of an enterprise security risk management (ESRM) approach which emphasizes risk principles (vs functional competencies) to managing security risks. – Josh Massey, Department Manager at MITRE*

According to Brian Allen, an ESRM evangelist, "When ESRM principles are applied, the security function changes completely – from a set of tasks, performed discretely, to a role. ERSM means security decisions are made by the right person, with the right authority and accountability, and for the right reasons – reasons based on defined risk principles."

So, what does a collaborative approach look like?

To adequately describe a proactive insider threat solution based on the cooperation of both physical and cyber teams, we first need to establish a foundational understanding of who insiders are, what an insider threat is defined as, and lastly, which pre-incident indicators of insider threats are most detectable. For this, I will reference baseline definitions provided by the United States Cyber & Infrastructure Security Agency (CISA).

Who are Insiders? According to the CISA, insiders are described as any person who has or previously had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, and systems. Examples of an insider include the following:

- A person the organization trusts, including employees and those to whom the organization has given sensitive information and access.
- A person is given a badge or access device identifying them as someone with regular or continuous access.

- A person to whom the organization has supplied a computer and/or network access.
- A person who develops the organization's products and services.
- A person knowledgeable about the organization's business strategy and goals, entrusted with future plans, or the means to sustain the organization.
- In the context of government functions, the insider can be a person with access to protected information, which, if compromised, could cause damage to national security and public safety.

How to Define an Insider Threat? The CISA defines insider threat as "the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems." This threat can manifest as damage through the following behaviors:

- Espionage
- Workplace violence
- Terrorism
- Sabotage & unauthorized disclosure of sensitive information
- Intentional or unintentional loss or degradation of departmental resources or capabilities
- Corruption, including participation in transnational organized crime

Pre-Incident Indicators of Compromise

Lastly, let's describe some of the most notable pre-incident indicators or detectable symptoms of insider threat. In his book "Beyond Fear," security expert Bruce Schneier discusses the motivations and behaviors of malicious insiders. Schneier reminds us that detecting a malicious insider attack can be extremely difficult, particularly when you're dealing with a calculated attacker or a disgruntled employee who knows a great deal about your company. One way to detect such an attack is to pay attention to the various indicators of suspicious behavior, which include both digital and physical indicators, some of which are listed below:

- Poor performance appraisals
- Voicing disagreement with internal policies
- Disagreement with coworkers
- Financial distress or unexplained financial gain
- Unexplained travel patterns
- Odd working hours or a hasty departure from the company
- Attempting to access restricted areas of the company network
- Data offloads
- Failure to complete mandatory security training

The Common Insider Threat Investigation Scenario

Now that we have a baseline roughly defined let's play out a typical scenario using a collaborative approach with the data, tools, and techniques available today. In the following insider threat use case, it is noticed via a user activity monitoring system that an employee (Bob) repeatedly attempts to access a restricted part of the corporate network. To gain the best intelligence, we need participation from the right people with the right mindset, implement a unified process, and adopt appropriate supporting technology.

As security intelligence professionals, we need to determine if the individual is a credible threat to the business. To accomplish this at scale, we need to kick off a workflow that will allow us to discover other pre-incident indicators of insider threat so we can add context to the indicators of compromise that triggered the concern in the first place. As we cultivate that intelligence, we need to properly assess if this person was just having a bad day or are they fitting the known behavioral patterns of a malicious insider.

A Typical Genesis | SIEM Alert – This is the network's user activity monitoring alert that says Bob recently attempted to access a compartmentalized part of the network he once had access to for a special project. It appears that Bob used two-factor authentication when attempting to access the network multiple times from the company IP address. Corporate access control data shows that Bob was in the building at the time of the incident. So now what?

Bob is interviewed and mentioned that he just needed to get a file to reference for a prior project. If we are satisfied with the answer, that's where the investigation could possibly end. We have seen this happen many times. But as we uplevel our threat-hunting game, we want to see what the proper convergence of cyber and physical data could tell us.

The insider threat investigation workflow referenced below is relatively similar to the one we covered in the Protector's Guide to Establishing an Intelligence Baseline. This one, however, will require deeper access to your company's legacy data and a greater level of participation from the right teams to successfully implement. As with the workflow in the Protectors Guide, these are suggestive outcomes you are looking for, not prescriptive steps. We understand that all teams have a work style that varies and take that into account when moving through the workflow.

Resolve the identity of the potential threat actor – With an insider threat case, this is typically much easier than an external actor, which operates in the shadows. We still must ensure that we are tracking the right individual (or individuals) so that a proper investigation can be conducted. If you fail to consider that an individual has multiple identities, uses a subtle alias, maiden name, etc., your investigative results may be skewed and the bigger picture may be missed.

Scan company systems for internal data – This is where full cooperation from physical, cyber, legal, and HR will transform your results. This means checking all known incident reports, investigations, and observations, as well as data logs of access control systems, including license plate readers, arrest record feeds, and other systems of record to see if there have been any issues associated with this employee in the past. We are looking for anything that indicates that the person was involved in a hostile interaction while on company property, attempted to access the corporate facility off hours, had behavioral issues or other indicators of risk. This data is critical, and it is most likely already stored in your company somewhere. Access to it will allow the analyst to know quickly if this is a net new issue or a critical indicator of a newly discovered threat.

Public records / OSINT – This is the area that seems to be under-leveraged or misunderstood. To benefit from the value of this information, the right approach to OSINT and public records needs to be coordinated. I promise that it's as important as any other step in this workflow. It's inexpensive, it can be driven with SOPs so it is highly scalable and somewhat automated, and it may generate a wealth of information related to the background of the person of concern. We want to know about civil litigation records, criminal history, and financial-related cases such as collections issues, bankruptcy, liens, judgments – even evictions and foreclosures. We want to see if there is a potential motivator for financial gain or other ongoing issues that may incentivize or trigger malicious behavior. Additionally, with a proper OSINT scrub, to include an adverse media search, we can determine a person's mindset, mode of living, affiliated interest groups, and determine what their standard behavior looks like.

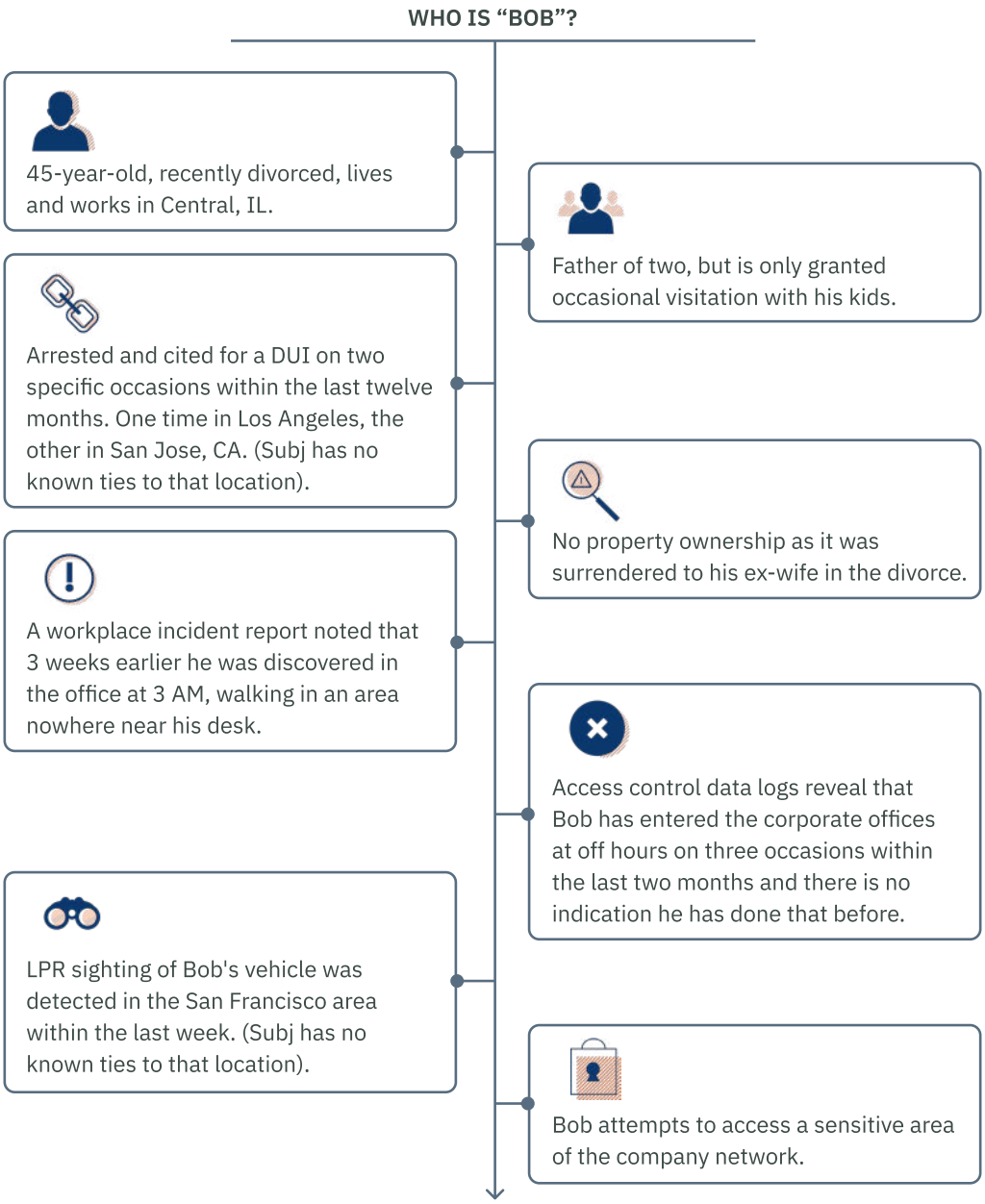
Initiate an investigative assessment – We need to collect the right information and quickly discover anomalies or other patterns that are concerning. We are looking to see if any of the original IOCs / PINs now appear more serious or can be explained away by other factors. Just as there are assessments geared towards workplace violence, there are also formalized insider threat assessment rubrics that can generate risk scores to determine the likelihood that someone is a potential risk for insider threat. This is an area that can generate the proper "what next" for the investigator and create broader defensibility for the organization.

Alert proper teams, gather & share intel – We need to work closely with other departments, including legal, HR, campus security, or even law enforcement if deemed necessary. During this step, we are both cultivating more information that may lead to actionable intelligence and making others aware of what they need to know to shore up their infrastructure. There may be an overlapping issue that can be discovered if the proper teams communicate effectively. Just like the investigative workflow for determining pre-incident indicators of risk, this step can and should happen early and often in the investigative process. It does not have to happen in sequence with other steps.

Establish or recalibrate protective strategies – This is where the complete picture is analyzed and the decision is made to either close out or escalate the investigation, implement in-depth monitoring, or even exploit the threat to determine if it's associated with a larger party of threat actors. A lot of this will depend on legal constraints, company culture, and sensitivities, as well as the business's acceptable level of risk.

Context is Key

Successful investigations require art, science and decades of experience, which include the development of a gut instinct to keep running down a lead. No checklist can replace that, and we would never attempt to over-standardize a process as sensitive as this. But as we demonstrate a connected workflow where the right people can quickly generate the right information, imagine a scenario where the following information is what we find on the fictitious character Bob. Then ask yourself: how would the urgency heighten, and would your monitoring and mitigation strategy change?



Understanding the Bigger Picture

With a holistic threat detection approach, we can now layer in all pertinent information to more accurately understand the evolution of the insider threat. Just like with physical threat indicators, we can uncover potential trigger events in a threat actor's life, e.g., anniversary of termination, a death in the family, or perhaps a tense legal case involving a divorce or financial issues. By surfacing this type of information and comparing it to the digital signals and indicators that cyber teams have access to, insider threat intelligence teams can more accurately determine the bigger picture and mitigate the threat quicker than ever.

As we continue to dissect the evolution of the insider threat, it is evident that these investigations do not rely solely on cyber systems and tradecraft. Many physical intelligence teams uncover behaviors that allow us to recognize a pre-incident indicator of risk. These pre-incident indicators or indicators of compromise can be generated through human intel, incident reports, anomalous behavior in access control & visitor mgmt systems, license plate readers, as well as data gleaned from continuous monitoring involving criminal activity. This is why collaboration between teams is so critical.

Is it overly idealistic to think that a CISO and CSO will join forces to mitigate insider threats? I don't think so. I see the capabilities we have in front of us, and the culture shift is gaining momentum. As organizations start to tear down silos, they are getting a much broader picture of the insider risk landscape. Security intelligence and cyber teams are not locked in a zero-sum game. In fact, they have much to gain by collaborating because they face identical challenges, which are occasionally driven by identical threat actors. If we can work together to proactively identify, disrupt, and, most importantly, prevent an insider threat actor before they are successful, we have achieved an important victory.

Strengthening Insider Threat Resilience with Cyber-Physical Integration

By: Tom Kopecky

This article was written in partnership with Josh Massey, Director of Enterprise Risk of The MITRE Corporation's Enterprise Security Assurance department. As such, Mr. Massey is responsible for establishing, executing, supervising, and directing the implementation and oversight of MITRE's insider threat program and strategic protection initiatives across MITRE's six federally funded research and development centers in the fields of defense & intelligence, aviation, civil agency modernization, homeland security, healthcare, and cybersecurity.

In part one of this two-part overview, we addressed many of the key themes and priorities required to properly fight the battle against our common enemy, which we callout as insider threat or insider risk. There has been a great deal of discourse relating to how an organization's program can blend cyber and physical security intelligence operations to realize the outcome that we all hope to achieve. In this article, we want to dig in at a tactical level to show how this is achieved. It's much more than having the right people, process, and technology – it's critical also to recognize nuances of your business, including the vertical you are operating in, the company culture, and legal compliance requirements – which will ultimately limit your ability to get creative.

We often find that many organizations already have the bulk of the required information, data, and personnel to lay the groundwork for an insider threat program – they just need guidance or operational templates to start the process tactically. As important as the "how to" is the "why should we," and that is why you'll require support from the entire organization from the C Suite, including Chief Legal, Risk, Human Resources, and more.

Lastly, it is essential as you consider your program development priorities to be able to point to nationally recognized standards. As a security leader, you can use these standards, compliance regulations, documented best practices, and benchmarking to help secure the proper approvals and create defensibility for your company's action plan. Remove the onus from yourself having to prove why this is so important to implement and point to recognized methodologies. This will help educate key stakeholders and also help minimize the negative stigma that leadership may have about insider threat intelligence operations.

The Mindset

I spoke to Josh Massey about his methodologies and strategic mindset when implementing an insider threat program, and he had this to say "...We either win together or lose together. At MITRE, we've structured our insider threat program to eliminate the artificial, functional turf wars of security silos in favor of an enterprise security risk management (ESRM) approach."

So, how do we start with the ESRM approach, and what standards do we use to lay the program's foundation?

Several models and frameworks provide solid foundations for understanding ESRM concepts and how to apply them across security domains, enabling greater confidence from your C-suite and then adapting to your vertical and organizational culture as needed.

For example, within the insider threat domain, the National Insider Threat Task Force (NITTF) has promulgated a maturity framework, and while it's interesting to note that although this framework is meant to model a government agency's program, numerous pieces can also be applied to the private sector. Some of the elements called out by the NITTF maturity framework are quite relevant to an ESRM mindset:

Maturity Element 2: Employ metrics to determine progress in achieving program objectives and to identify areas requiring improvement.

Maturity Element 4: Employ risk management principles tailored to address the evolving threat and mission needs.

Maturity Element 5: Include stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen the InTP processes.

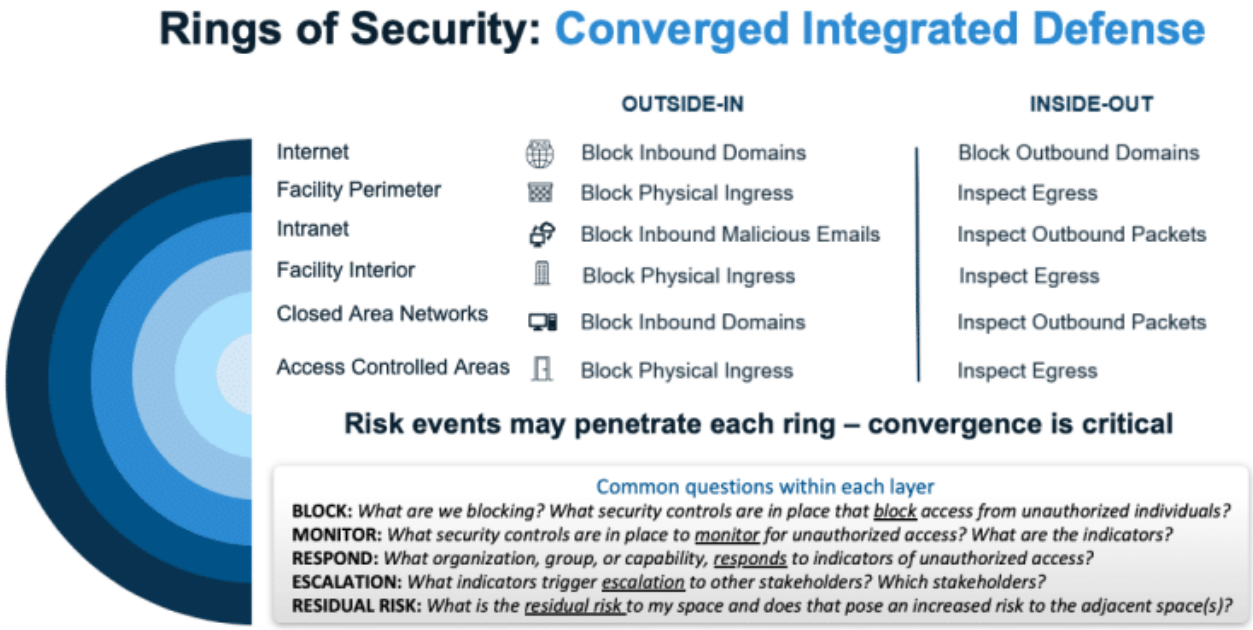
Getting Tactical

Since we operate in organizations that often have disparate functional elements of security, we must figure out how to bridge the application of a more generalized framework with the practical needs of driving convergence across these security disciplines and domains. Let's look at how we can take an ESRM framework and model it to work more effectively within a corporate environment.

For this, I again relied on the expertise of Josh Massey from MITRE to articulate some of the key considerations his team looks for when building and implementing a program. Josh and team have teased out a framework that is more relevant to the environment most of us are operating. It also supports one of the key takeaways in Ontic's 2022 Mid-Year Outlook State of Protective Intelligence Report, where we note that a common problem is related to communication silos and how they continue while different departments assess the same threat individually. This increases the likelihood that security decisions are being made without complete information.

MITRE Converged Integrated Defense Framework

Principally, cybersecurity and traditional security domains can and should be viewed holistically as interdependent "rings of security." When viewed in this converged manner, an organization is better postured with an integrated defense.



Many security domains understand the concept of "security in depth" within their domain but probably have never considered the value and impact of a converged, integrated defense that provides "security in depth" across multiple disciplines.

For the sake of this discussion, we will focus on the convergence of the physical and cyber domains. At a strategic level, a converged or integrated outlook would ensure a much higher level of security. At a tactical level, it would enable tradeoffs in and at each domain as you become more aware of the supporting elements within the other domain. This more inclusive approach will inform where more robust protections are most needed.

For example, as you move "inward" to your most valued resources, tradeoffs become more impactful and should be considered with greater scrutiny. What is most interesting from viewing security in this matter is the realization that protections can operate across two spectrums: an "outside-in" view protects from external threats and "penetrations." In contrast, an "inside-out" approach protects from trusted insiders and "exfiltration." With this mindset, a much richer debate can occur over the value of any security control or mitigation

An "Outside-In" or "Inside-Out" Approach

So what do we mean by this "outside-in" or "inside-out" approach? Consider a converged or integrated defense as "rings of security" that provide "security in depth." What makes it a converged or integrated model is that these rings do not represent one domain but multiple domains. In this example, the alternating cyber and physical "rings of security" from the outside in would look like this:

- **Internet Perimeter:** Think of firewalls as your outermost "fence line," which protects against unauthorized intruders from around the world.

- **Facility Perimeter:** Your fence line or facility boundary is the outermost physical security boundary, and while still accessible by the public, any unauthorized intruder must be physically present at that location.
- **Intranet:** This is the common network area accessible only by "trusted insiders," but it is accessible by all trusted insiders.
- **Facility:** Similarly, internal access to common facility areas is accessible only by "trusted insiders" but accessible by "all" trusted insiders.
- **Closed Area Networks:** Information the organization deems sensitive or that warrants enhanced protection is controlled via closed area networks and is accessible only by a subset of your trusted insider population.
- **Access-Controlled Areas:** Similarly, physical areas or resources the organization deems sensitive or warrant enhanced protection are protected via access-controlled areas accessible only by a subset of trusted insiders.

Each "ring of security" asks and answers the same fundamental questions but in accordance with different risk tolerances. A converged model also allows considerations of "tradeoffs" due to a more nuanced understanding of the security controls and mitigations across either adjacent ring.

The common considerations across each ring include the following:

- **Block:** What are we blocking? What security controls are in place that "block" access from unauthorized individuals? Just as important to understand, what are we still letting through, or what is the residual vulnerability to an adjacent ring?
- **Monitor:** What security controls are in place to monitor when unauthorized accesses are blocked and/or if a control is bypassed and an intruder can gain unauthorized access?
- **Respond:** What organization, group, or capability responds to unauthorized access at this ring? If multiple elements have a response responsibility, how do those elements communicate and share their alert response actions and findings?
- **Escalation/Collaboration**: Who are the other stakeholders who may have the capabilities to support a response or should be notified of the primary response to be better informed of potential risks for their assigned space? Is there a platform or capability to document and track risks across spaces in a more unified manner?
- **Residual Vulnerability:** What is the residual risk to my space, and does that pose an increased risk to the adjacent space(s)?

As mentioned in part one, security should not be viewed as a zero-sum game across/between security domains. We are not in competition with each other but instead are on the same team against a common adversary. The more we can begin to consider the resources and capabilities we each have in an integrated defense model, the quicker we can move towards a converged state where risks are understood and effectively mitigated against any threat that may emerge from outside or within our organizations.

Protective Intelligence Within Executive Protection

As threats in the world become more resourceful, diverse, and determined along their pathways to violence or to inflict harm, executive protection (EP) practitioners must increasingly shoulder a heavier burden. It is no longer acceptable for protection managers and their consumers (protectees – those being protected) to rely on the reactionary expertise and capabilities of the protector. Therefore, proactive Protective Intelligence (PI) programs must be integrated as an essential part of the EP mission. To accomplish this, two primary problems require resolution.

First, protection managers must be able to justify the necessity of PI, quantify the program's value, and then harness the necessary buy-in from the EP customer. Second, protection managers must understand how to best utilize and disseminate the products created by the PI program.

Many experts in the field of Protective Intelligence have advocated and written about the benefits and value of a PI program. Literary works by subject matter experts such as Fein, Vossekuil, Calhoun, and Weston study the process of identifying and managing threats. Companies and organizations such as Ontic Technologies, Torchstone Global, and Emergent Risk International publish a steady stream of articles that focus on PI's processes and advantages in the EP and corporate security arena. However, there is little information to guide the EP manager, who leads a small team with limited budgetary resources wishing to implement a PI program. There is also a lack of material regarding the individual EP practitioner's most effective and efficient use of intelligence products.

Although much has been written about PI, its practice still resides predominately in large corporate security and EP programs – those who can afford it. This effort aims to identify useful information and provide insight so that EP teams, regardless of size and budgetary restrictions, can implement and utilize PI. The goal is to increase the EP team's operational effectiveness, to allocate limited resources more efficiently, and to increase the value of EP services provided to the customer.

The Foundations

Protective Intelligence is a relatively new practice in the executive protection industry, at least relative to the reliance on intelligence work to support national defense and homeland security goals. Protective Intelligence has been built on the foundations of national intelligence and law enforcement intelligence but tailored to meet the needs of the executive protection mission. There have been volumes written about every facet of national intelligence, and a great deal has been written about intelligence efforts to assist law enforcement. However, little information has been published regarding the use of Protective Intelligence in the executive protection arena.

Protective Intelligence within executive protection encompasses, or sometimes falls within, three broad skill sets: the intelligence production process, threat assessment and management, and risk assessment and management. There are many published works on these subjects, and to understand how Protective Intelligence applies to executive protection, one must first study all three. Only after thoroughly comprehending these three subjects will an executive protection manager know how to incorporate the benefits of a Protective Intelligence program and then how to successfully operate and maintain the program.

The Role of Protective Intelligence in Estate Security

Estate security is critical for corporate executive protection teams and their supporting Protective Intelligence programs. We realize that executives spend most of their time at the corporate office, their primary estate, and various travel destinations. Two of those are static locations and are often desirable targets for would-be attackers or inappropriate pursuers.

A static target affords the would-be attacker the benefit of predictability in location and personnel, observing a private estate security team's standard operating procedures and shift changes, vulnerabilities based on observable patterns, and more. The good news for security is that this is a double-edged sword for the adversary because for them to successfully approach an executive or the estate, they must conduct pre-operational surveillance — forcing them to venture within the eyesight of security, thus becoming vulnerable to detection.

A fundamental piece of the Protective Intelligence puzzle is directly observing potentially malicious activity. It is well known that pre-operational surveillance can be detected early by agents of estate security services or counter surveillance teams that are switched on and trained to detect patterns of hostile surveillance or other pretext site visits. Even executive assistants and domestic and household staff often act as the eyes and ears of the security program. They can identify anomalies and professionally challenge those who appear out of place.

Estate security systems fulfill a critical Protective Intelligence function by acting as a static post and base of operations for many protective movements. Agents charged with providing estate security management can proactively observe, identify, assess, and understand what is normal and can quickly determine an anomaly. Based on the vast knowledge of the security professionals protecting the estate, they can compare activity at the moment to their baseline, developed over hundreds of hours of observing activity in that area. Using their baseline as a standard, they can discriminate between ordinary activity in the environment and that which needs to be investigated further.

Estate security professionals collect enormous information on various people, incidents, and activities. Data that is typically collected or observed includes, but is not limited to the following:

- Local criminal activity and trends
- Suspicious people & vehicles loitering in the area (i.e., what is a known vendor or contractor vs. potentially hostile surveillance)
- Vehicle license plate data obtained by visual observation or ALPR systems
- Attempted contacts with the principal by inappropriate pursuers or by those posing as a legitimate business engagement (in-person or via US mail)
- Heightened interest in the principals, which may be currently driven by media, further escalates the client's threat profile
- Corporate-related incident / investigative reports that reference resentful employees and related workplace issues

The amount of data an estate security program can collect when it operates 24 hours per day for years cannot be illustrated in several bullet points. (But our readers already knew that)

Protective Intelligence Challenges in Estate Security

Security intelligence data can be our best friend or worst enemy. On one hand, it enables Protective Intelligence analysts and security personnel to discover patterns and relationships between key events, people, and entities. However, when data becomes unmanageable in size after years of collection, it loses utility. What good is security data if it's a headache for the analyst to sift through?

This leads us to one of the biggest problems identified among Protective Intelligence teams: How does one quickly analyze years of security intelligence data? How do professionals tasked with providing security for a client know about every piece of information collected over the years to determine its relevance now?

Second to the data analysis and management problem, estate security solutions face the challenge of information sharing: Is there an appropriate flow of information between groups responsible for most of the executive's security coverage (i.e., estate security and corporate security teams)?

It's the age-old challenge of information sharing. Every executive protection team must find the right balance for their situation. Arrangements of proprietary/contract/hybrid security at the estate, the corporate office, and other sites can make information sharing complicated and restrictive due to the sensitivity of confidential information. Consider the questions below:

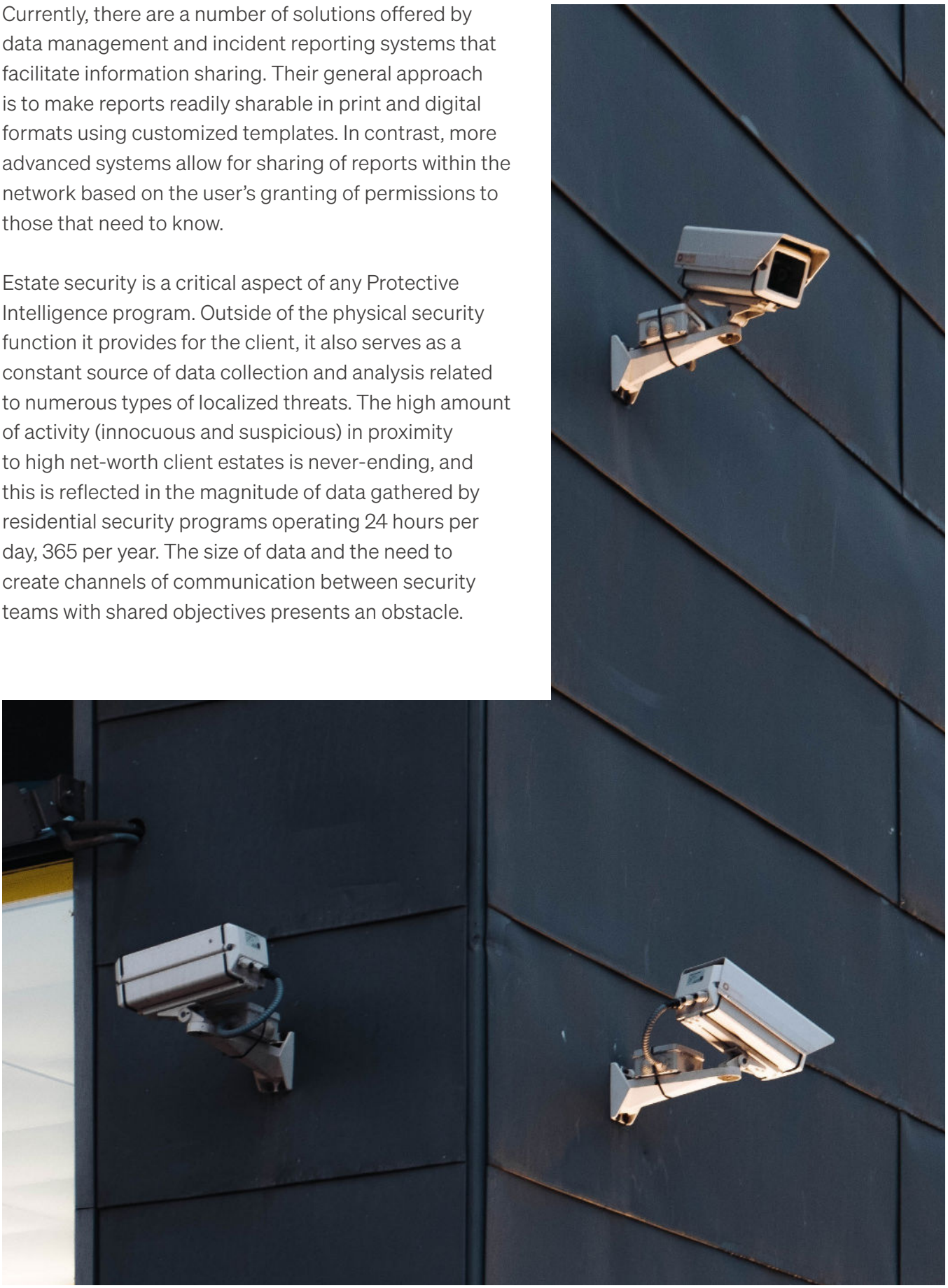
1. Will information sharing between the estate security team and the corporate security team reduce overall risk to the executive?
2. Who will the information be shared with? (liaison)
3. How will information be shared? (medium)
4. What is the likelihood/impact of the information being compromised by negligent security practices?
5. How can a security team ensure that peripheral support departments and staff help by driving more valuable information to the primary data set without also having too much access to that same data?

These are important questions to ask because some of the largest security companies in the US (by revenue) utilize guard force management to support corporate facilities, and the risks of sharing sensitive information with non-proprietary contract "guards" must be weighed carefully.

Those considerations aside, it is a win-win scenario to have open communication channels between trusted, competent security teams, especially when sharing important Protective Intelligence information. Consider this: if a pursuer approaches the corporate office, there is certainly a heightened probability that they will eventually attempt to approach the executive's primary or secondary residence — communication between departmental teams is crucial.

Currently, there are a number of solutions offered by data management and incident reporting systems that facilitate information sharing. Their general approach is to make reports readily sharable in print and digital formats using customized templates. In contrast, more advanced systems allow for sharing of reports within the network based on the user's granting of permissions to those that need to know.

Estate security is a critical aspect of any Protective Intelligence program. Outside of the physical security function it provides for the client, it also serves as a constant source of data collection and analysis related to numerous types of localized threats. The high amount of activity (innocuous and suspicious) in proximity to high net-worth client estates is never-ending, and this is reflected in the magnitude of data gathered by residential security programs operating 24 hours per day, 365 per year. The size of data and the need to create channels of communication between security teams with shared objectives presents an obstacle.



Working Smarter to Protect Family Offices and High Profile Individuals

No detail is too small when evaluating the activity that surrounds high-profile individuals and their families. Whether it be their morning coffee shop routine, their children's activity level on social media, or how to keep an appropriate distance from crowds at philanthropic events, there is a great deal of risk to mitigate daily.

We must work harder to protect
The ability to capture information on high-profile individuals, especially those more public-facing, constantly expands. This makes the ability to access sensitive information much easier. This is why it's important to reverse engineer things and put yourself in the place of the threat actor to figure out, 'What, what steps would I take if I were the bad guy to get into the world of this protectee?'

It's critical to stay one step ahead of the most creative adversary. It's not easy, but with processes and technology that spot and surface warnings, teams can work smarter to avoid everything from small issues to worst-case scenarios.

Force multiplier — How are you spending your time?
Every minute of the day matters in ensuring your principal's physical and online presence is protected and their surrounding family and staff. When teams can automate many tasks like monitoring threat activity or unknown vehicles on the perimeter of a residence, they can spend valuable time being the eyes and ears of the protection unit versus being buried in data.

Often, "teams" are comprised of one individual supporting not only the main principal but their family as well. Knowing your process can easily scale and adapt to changes in team structure and new threats (i.e., health and safety) is critical because we know that a family office is a business, and it must adapt to economic changes.

Automation — Are you relying on hard copies and Post-it notes?
Connecting the dots becomes increasingly challenging with binders and notebooks of threat documentation. Having the confidence to report that a threat was a random act and not connected to historical activity (prior threat actors) is one way to ease the pressure that comes with the territory of protecting others 24/7.

There are ways to manage online presence and ensure intelligence is always on, such as training principals and their families on the risks associated with social media, watching news and media cycles, and automating threat activity as soon as it arises.

Privacy and discretion — Are you looking for signals to protect against larger threats?
Family offices require the utmost level of privacy and discretion in their day-to-day operations, as even the smallest data point of a principal's routine can lead to uncovering more.

Kidnapping is a threat that often drives many personal security decisions; however, as Fred Burton, Executive Director of Protective Intelligence, shares, “Threat of kidnappings is very low for high-net-worth families and CEOs within the United States. I believe these kidnapping fears are not based on facts but driven by perceptions and the media interest surrounding historical cases.”

Strategizing for a worst-case event often involves planning that takes months or years to execute, so it’s important to constantly look for signals of what doesn’t look or feel right. Stalking is also a common threat against high-profile individuals and can sometimes lead to a more violent course of action.

SECTION V

Case Studies: Protective Intelligence Successes and Failures

Unraveling The Michigan Plot

By: Fred Burton

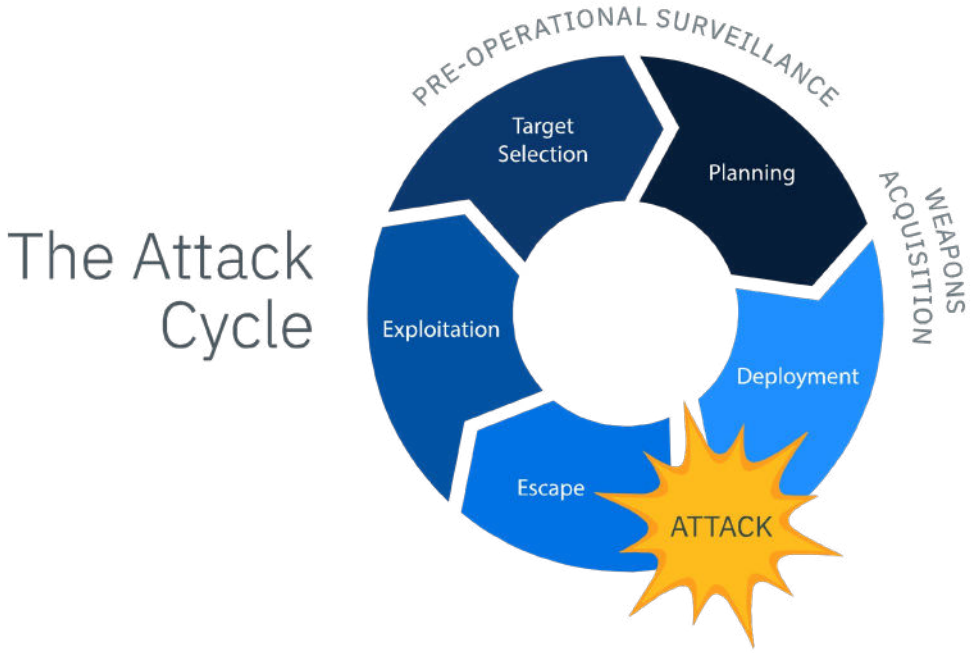
In October 2020, thirteen men were arrested and charged with plotting to kidnap Michigan Governor Gretchen Whitmer. The cell also looked at targeting law enforcement personnel, plotted civil unrest, and discussed attacking the State Capitol of Michigan. At the same time, later information indicated the group also considered targeting Virginia Governor Ralph Northam. One of the arrested suspects was a former Marine who worked for a security company. (source: Detroit Free Press) Fortunately, the FBI had infiltrated the group based on its earlier threats against law enforcement personnel and was monitoring their attack plans.

Even though the plot was more aspirational than operational, the case is very instructive for those of us engaged in the tradecraft of protection. As a student of protection history, I can't recall another case in which two state governors were targeted for kidnapping. That in itself is unique. In fact, the case is a textbook example of an effective Protective Intelligence investigation. (source: Reuters)

Looking at the information available about the case, there are a few key takeaways that protection professionals should understand and build into their programs.

Pre-Operational Surveillance is Only Visible If You're Watching
Tradecraft-wise, pre-operational surveillance actions have always been key in my mind in stopping the attack cycle. This cell was operational when they conducted a reconnaissance of the Michigan governor's summer residence. As I think about this plot, I question whether or not the protective details and police would have observed the surveillance actions of those involved in the plot, absent the intelligence developed by the FBI?

Surveillance detection works if you know what you are looking for, aided by training and technology tools. As far as I'm concerned, it's the most cost-efficient manner of protection in the industry. If you don't have a surveillance detection program, this plot reminds you of the importance.



Technology can also help your team watch for and evaluate potential threats. In this plot, the affidavit says members of the group drove by the Michigan governor's residence in Lansing and her vacation homes numerous times while also conducting surveillance by boat from the waters near her vacation home. Technology, such as license plate readers, can be used to identify unusual vehicles near the protectee. At the same time, robust databasing and analysis capabilities can help to determine whether these passes are unusual or coincidental.

Attackers Understand When and Where Your Protectee is Most Vulnerable

Even though this group of attackers was largely aspirational, their framework for conducting surveillance was sound. It provided substantial details about Governor Whitmer's activities and the best locations for a potential attack. According to the affidavit, the group had decided that, based on their surveillance activities, "their best opportunity to abduct Governor Whitmer would be when she was arriving at, or leaving, either her personal vacation home or the Governor's official summer residence."

There are two dangerous aspects of this issue to consider:

1. The group was very cognizant of the times when the governor would be most vulnerable to an attack, and they built their plans to coincide with the most critical times.
2. They understood that security measures may be more lax at a vacation home compared to the normal work environment. They made plans on that basis, raising the chances for a successful kidnapping operation.

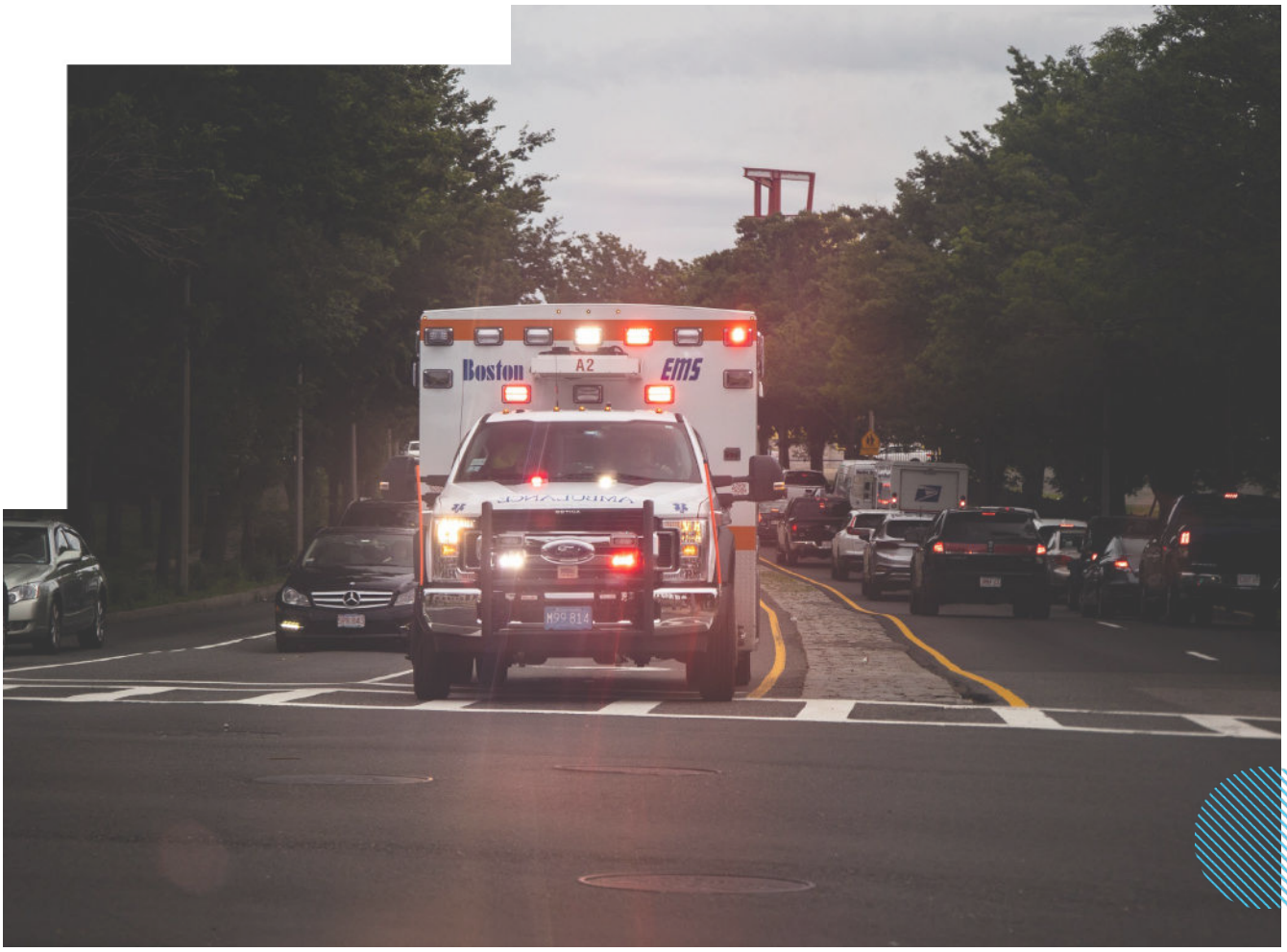
In this business, vacations and off-duty hours pose unique protective security challenges for protection details. This is especially true for VIPs seeking less security than they would in their normal work and home environment. This case is a vivid reminder of why threat assessments need to be constantly evaluated. Just because a protectee is on vacation doesn't mean the threat has diminished. On the contrary, that's the time any good (or even bad) surveillance team would see that security has been reduced.

Attackers Are Planning For Secondary Attacks. You Should Too.

One of the more interesting parts of the bigger-picture analysis of this plot was the group's plans to attack secondary locations to slow down first responders, reportedly including plans to blow up a nearby bridge or throw Molotov cocktails into police vehicles. This was a novel idea and a reminder of something rarely looked at in threat assessments. Some questions to consider include:

- What are the response times in various locations for fire, police, and EMS?
- What could slow down first responders?
- Is your team prepared to handle the initial fallout from a potential attack if first responders are delayed?
- Is there a safe haven in the vacation home?
- Do you have a trauma kit and Stop The Bleed supplies?

In this case, the plotters were infiltrated by the FBI, who was relentlessly monitoring their activities and stopped the group before it took action. For protection professionals, it's critical to ensure your team is taking appropriate action to find surveillance, use technology where possible to support your efforts, maintain appropriate security measures in all areas, and reevaluate your response plans for any attacks that law enforcement might not spot in time.



The Delivery Man Ruse: An Effective Method To Kill

By: Fred Burton

After a lifetime of examining attacks and failed plots, my eye has always been drawn to the "how" of the attack rather than the "why." Don't get me wrong — the "why" is important for analysts and prosecutors but not so much for the protectors or those charged with stopping the attack before it occurs. Why is that? Because if you can understand how an attack has been put together and what factors made it possible, you can do something to mitigate that threat going forward.

One of the basic tenets of any Protective Intelligence investigation or after-action study is to figure out the "how." Frankly, it's the only way you can stop an attack from occurring. Federal protective agencies like the U.S. Secret Service and the Department of State's Diplomatic Security Service have learned this lesson the hard way over the years.

One tactic I've seen several times over the years is known as the "delivery man ruse." Sadly, we saw this tactic employed successfully again on July 19th at the New Jersey home of a U.S. Federal Judge. In this case, the attacker disguised himself as a FedEx delivery man and reportedly carried a FedEx package when he arrived at the door. The attacker opened fire on the judge's husband and her 20-year-old son. Her son died of injuries sustained during the attack, and her husband was critically injured.

I first considered this specific ruse in 1975 in reading James Grady's brilliant thriller-turned-film called "Three Days of The Condor," starring Robert Redford and Faye Dunaway. I've had the privilege of knowing and speaking to Jim for a podcast; his insights are fantastic. I saw the tactic used in real life in 1980 while I was on the scene of a transnational act of terror as a young EMT with the Bethesda-Chevy Chase Rescue Squad. The gunman — disguised as a mailman and using a stolen U.S. Postal Service jeep — shot and killed an Iranian dissident at his front door. I would later hunt for that killer as a special agent, but we were too late — now he's hunkered down and safehaved inside Iran. I suspect he may have gotten the idea for the ruse by watching the Hollywood film or reading Grady's book.

In the latest case in New Jersey, the shooter (who we will not name) was a lawyer who had previously appeared before the judge he targeted. According to information found after the attack, the shooter died of a self-inflicted gunshot wound. He was fixated on revenge and had a targeted kill list. It later became clear that he had also killed before, murdering an attorney in California a few weeks earlier. He was a poster child for madness.

As threat hunters, our challenge is finding these stalkers and killers before they strike, but let's first examine the challenges the protectors and analysts faced in this situation.

According to the U.S. Marshals Service, the Judicial Security Division is responsible for protecting about 2,700 judges and another 30,000 federal prosecutors and other court officials.

Case Study: Nasim Najafi Aghdam, Youtube Headquarters Shooting

By: Virginia Simmons and Tom Kopecky

Background

In 2018, Nasim Najafi Aghdam wounded three people at the YouTube Campus after entering an exterior parking garage and reaching an outdoor patio where she started firing. Nasim, an immigrant of Iranian descent, was motivated by perceived "discrimination" by YouTube for filtering and demonetizing her videos. Nasim routinely posted bizarre content on YouTube and other social media channels, including Facebook, Instagram, and Telegram, consisting of her beliefs and ideas regarding animal rights and veganism and her discontent with YouTube.

Nasim had no indications of prior alcohol or drug abuse, run-ins with law enforcement, or violence. In fact, family members described her as the opposite of violent, explaining that "she never hurt one ant, so how could she shoot people?" In addition, they stated that they didn't know Nasim had access to a weapon. It was not until a week before the attack that the family became concerned about Nasim.

On March 31st, the family reported Nasim as a missing person to authorities. She allegedly left her family due to troubles at home until she was found the morning before the shooting, sleeping in her car at a Walmart in Mountain View, twenty-five miles from the YouTube headquarters. At that point, she was never identified as a threat, even though her family warned law enforcement about her disappearance and her recent series of YouTube videos that expressed her anger with the company.

Synopsis

On April 3, 2018, at 12:46 pm in San Bruno, California, a 39-year-old, Nasim Najafi Aghdam, a female of Iranian descent, wounded three people with a 9mm Smith & Wesson semiautomatic pistol before shooting herself. Aghdam was reportedly upset with YouTube's practices and policies, including removing her videos. As a result, she decided to attack the YouTube Headquarters in San Bruno, California.

Nasim, also known as Green Nasim, was a vegan and animal-rights activist, bodybuilder, and artist. She routinely posted on four YouTube channels: one in Farsi, one in Turkish, one in English, and one in the form of hand art about her discontent with YouTube for filtering and censoring her videos.
The attack occurred at the YouTube headquarters, where Nasim fired indiscriminately at people she had no relationship with before shooting herself. Hours before the attack, Nasim visited a local gun range where she practiced aiming at targets with her legally purchased semiautomatic pistol. The first shots began around 12:46 PM and subsided shortly after Nasim died of a self-inflicted gunshot to the chest.

Timeline and Pre-Incident Indicators

1996: Nasim's family immigrates from Iran to the United States when she is 16. Her family finds a home in San Diego, California. (OCR)

2009: Nasim attends a protest for PETA in San Diego. She's quoted as stating, "For me, animal rights equal human rights." (SF Gate)

2010: Nasim becomes an active user on YouTube. Her four channels receive great attention, and she collects more than 9.2 million views over time. (Billboard)

2011: Nasim begins a non-profit organization called Peace Thunder. The business was eventually dissolve, and it is unknown if it earned any success. The company was intended to be an animal rights foundation. (Animal 24-7)

2013 (five years prior to the attack): Her family moves from San Diego to Menifee, CA, next to their neighbor, John Rundell. Rundell describes the family as "very, very friendly" and never recalls having issues with them. He did not see Nasim Aghdam in the months leading up to the attack. This is most likely because she was living with her grandmother in San Diego at the time. (USA)

February 2016: Nasim begins expressing discontent and frustration with YouTube, claiming that they were filtering and demonetizing her content. On her website, NasimeSabz.com, she complains that "when searching for [her] website in Google, at the top of the link they add 'an error occurred' but there is no error! They add it to keep you from visiting my site." (NY POST)

March 2016: Nasim posts a comment explaining that life is not good in the US. In a later video around the same time, she responds to viewers who have questioned whether she is mentally ill. She states, "I don't have any special mental or physical disease, but I live on a planet filled with disease, disorders, perversions, and injustices." (NY POST)

June 2016: Nasim begins experiencing a huge drop in views and subscribers from her main YouTube channel. She allegedly launched several more YouTube channels in the 2016-2017 time period, which also experienced drops in viewership. (Billboard)

January 2017: Nasim posts a video explaining that YouTube is "discriminating and filtering" her content.

February 2017: Nasim criticizes YouTube, stating, "There is no equal growth opportunity on YouTube." To further this rhetoric, she explains:

"There is no free speech in the real world, and you will be suppressed for telling the truth that is not supported by the system. Videos of targeted users are filtered and merely relegated so that people can hardly see their videos."

In addition, Nasim quotes Adolf Hitler, stating, “Make the lie big, make it simple, keep saying it, and eventually they will believe it.” (NBC Bay Area)

June 16, 2017: Nasim complains to YouTube about changes made on the site, specifically about views and revenue. (Billboard)

June 27, 2017: Nasim posts a screenshot of her email response from what appears to be the legal team at YouTube. Below the screenshot, she criticizes YouTube for discriminating against her and explains how she is experiencing a “huge drop in views” due to uploading her videos in Turkish and Farsi. (Billboard)

January 16, 2018: Nasim legally purchases a 9mm Smith & Wesson pistol in San Diego from a gun dealer in her name (SFGate).

February 20, 2018: YouTube begins “demonetizing” Nasim’s four channels. As a result of dips in viewership, Nasim does not earn a share of YouTube advertising revenue. (Animal 24-7)

March 31, 2018: The last time that Nasim was seen by her family. She was reportedly living with her grandmother in San Diego during this time. (Mercury News)

April 2, 2018: The brother and father of Nasim report her as a missing person from her hometown of San Diego, California. The two explain they are experiencing family problems at home but never express much concern for Nasim. (Business Insider)

April 3, 2018 – Day of the Shooting

1:40 AM – Mountain View Police find Nasim sleeping in her car in a local Walmart parking lot, nearly 25 miles from the YouTube Headquarters. However, after thorough questioning, Nasim did not appear to be a threat, nor did she ever mention YouTube in her 20-minute conversation with authorities.

2:00 AM – Officers leave Nasim. Shortly after, they return a call to the family to tell of Nasim’s whereabouts. In addition, they explain that Nasim was polite and cooperative and did not seem like a threat to anybody.

3:00 AM – Nearly one hour after the first call, Nasim’s father calls Mountain View Police to tell them she has posted a series of vegan videos. While he explains Nasim’s frustration with the company, he provides no information regarding a pending attack.

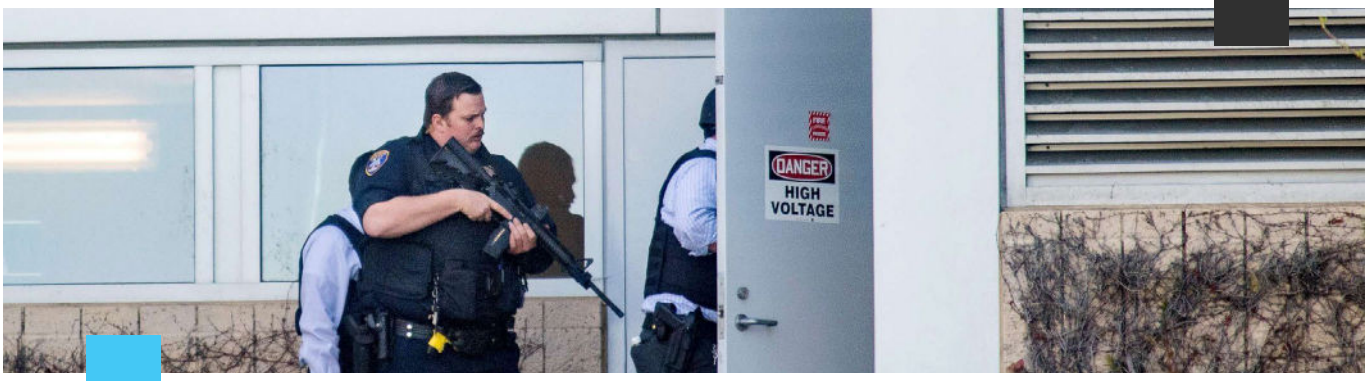
While the exact time is unclear, Nasim travels to San Bruno the same morning. Before she attacks the YouTube Headquarters, she visits a local gun range in San Bruno.

Around 12:00 PM – After she visits the gun range, Nasim drives and parks close to the YouTube Headquarters. She enters through an exterior parking lot and reaches an outdoor patio, where she begins shooting.

12:46 PM – Authorities receive 911 calls from people at the YouTube Headquarters reporting gunshots.

12:48 PM – Police arrive at the scene and begin their building entry. They find three victims with gunshot wounds and the deceased perpetrator, Nasim Aghdam, who appeared to have self-inflicted gunshot wounds.

Shortly after police arrive, the three wounded victims are taken to Zuckerberg San Francisco General Hospital. The two women victims are released that same evening, and by Thursday, the male victim is in "fair condition." (Business Insider, KQUED)



Summary of Findings

Nasim was born in Urmia, Iran, and immigrated to the US with her family in 1996. At the time, Nasim was in her late teens and struggled to assimilate into American culture. She continued identifying as "Persian" and speaking her native language, Farsi. The Aghdam family landed in San Diego, California, where they resided for several years.

There, they continued to practice the Bahá'í Faith, which originated in Dubai in 1950. While this religion has no dietary restrictions, Nasim frequently condemned meat eaters and supported the vegans who "aligned" with the practices of Bahá'í Faith. Because Shi'ite Islamists were the majority in Iran, followers of the Bahá'í Faith were frequently persecuted. It is most likely for this reason that Nasim and her family found refuge in the US.

When Nasim first became frustrated with YouTube (2016), the platform had implemented a new advertising policy that "demonetized channels with less than 1,000 subscribers and 4,000 hours of watch time." However, Nasim's English channel had over 5,000 subscribers and still appeared demonetized (Animals 24-7). As a result, Nasim and other vegan YouTube users began to protest against the company for not only demonetizing their content but censoring it too.

As Nasim's frustration with YouTube grew, so did her urges to do something about it. On January 16, 2018, Nasim legally purchased a gun from a dealer in San Diego. She later traveled to the YouTube headquarters on April 3, 2018, and shot four people, including herself.

Since the attack in 2018, all three victims have fully recovered.

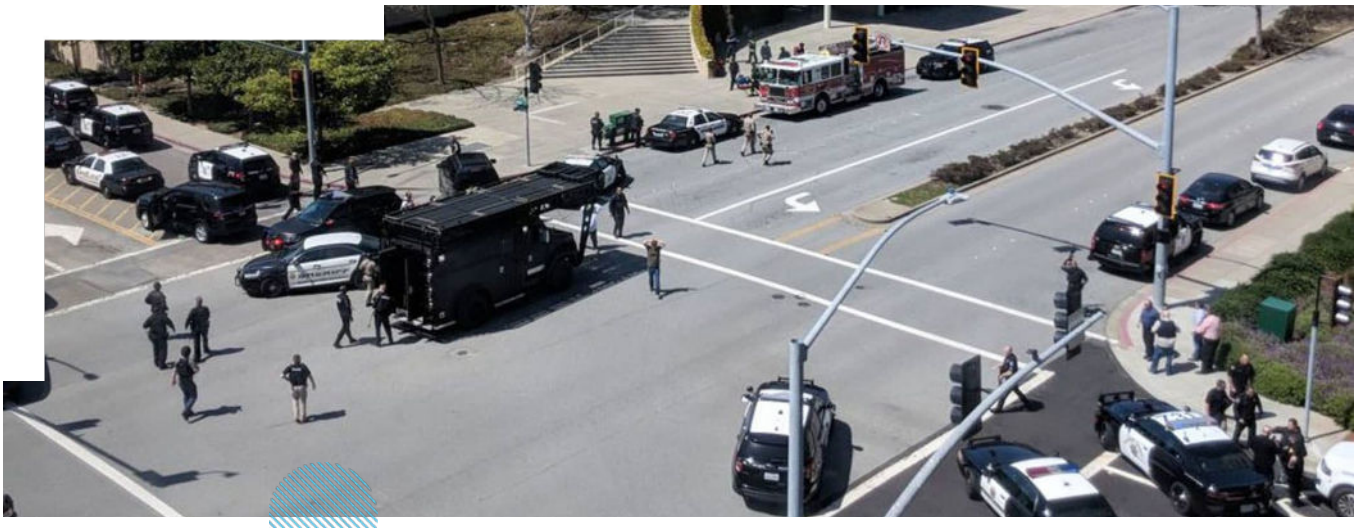
Pre-Incident Indicators

Pre-incident indicators resulting from human observation:

- In 2009, Nasim attended a protest for PETA dressed in a wig and jeans painted with blood drops for the protest.
- On January 16, 2018, Nasim legally purchased a firearm from a gun dealer in San Diego.
- In the months leading up to the attack, Nasim lived with her grandmother in Riverside rather than the rest of her family.
- In the time leading up to the attack, the family experienced conflict at home, but none indicating physical violence.
- On April 3, 2018, in the early afternoon, Nasim visited a local gun range in San Bruno, CA.
- March 31, 2018, is the last day Nasim is seen by her family.
- On April 2, 2018, Nasim is reported as a missing person by her brother and father.
- On April 3, 2018, authorities found Nasim sleeping in her car in a local Walmart parking lot in Mountain View, California (hours from her home in Menifee). She was released after questioning.
- On the morning of the attack, Nasim's father called authorities again to report that Nasim had posted a series of concerning videos.

Indicators that technology could have assisted with identifying:

- In 2016, Nasim began to display strange and erratic behavior in her videos. She was questioned about whether she was mentally ill by her viewers.
- In 2016, Nasim began posting content about her frustration with YouTube.
- Between 2017-2018, Nasim experienced a significant drop in viewership and subscription revenue.
- In 2017, Nasim emailed YouTube complaining about their new advertising policy. Shortly after, she posted a screenshot of their response online.



Case Study: Jared Lee Loughner, Shooting Of Rep. Gabby Giffords

By: Virginia Simmons and Tom Kopecky

Background

In 2011, Jared Lee Loughner killed six and wounded thirteen people at a public and scheduled event for U.S. Representative Gabrielle Giffords. Loughner was a high school drop-out with a history of mental illness, drug and alcohol abuse, a fixation on firearms, an inability to keep a job, and displayed bizarre and disruptive behaviors in the classroom. Loughner was very active in the online world, including postings of disturbing and threatening statements on MySpace and YouTube while referencing suicidal ideations and threats against police officers.

Loughner's fixation with Giffords began in 2007 after the two met at a community event. Allegedly, Loughner did not like the way Giffords responded to one of his questions, which culminated in the attack approximately four years later (reported by CNN). It doesn't appear that Loughner attempted direct contact with Giffords during that period, but it's unclear if he stalked her online.

Summary of Events

- On January 8, 2011, at 10:10 AM in Tucson, AZ, 22-year-old Jared Loughner, a Caucasian white male, killed six and wounded thirteen people with a Glock 19 9mm handgun. Congresswoman Giffords was the intended target. She was shot and wounded. (Reported by the Department of Homeland Security)
- Loughner had four magazines (two were extended 30-round magazines) and a knife on his person. The attack occurred at a public venue where Giffords had set up a constituent meeting in front of a Safeway supermarket. Loughner approached the tables set up for the meeting and began firing at 10:10 AM. All of the victims were shot during this time. The incident ended with the attacker being subdued by people attending the meeting at 10:15 AM. (Reported by Advanced Law Enforcement Rapid Response Training)
- Communications discovered after the attack indicated that Loughner may also have been seeking fame as an assassin.

Timeline of Pre-Incident Indicators

Summer 2005 – Before starting his junior year in high school, Loughner begins drinking and using drugs.

Summer 2006 – Loughner drops out of high school at the end of his junior year.

August 2007 – Loughner attends the "Congress on Your Corner" event in Tucson, AZ, with Rep. Giffords.

September 10, 2007 – Cited for possession of drug paraphernalia; charge dismissed after he completes a drug diversion program.

2008 (specific date unknown) – Loughner buys a 12-gauge shotgun from Sportsman's Warehouse in Tucson, AZ, and begins to exhibit signs of mental illness, such as hearing voices and communicating bizarre ideas.

October 13, 2008 – Arrested on a vandalism charge for defacing a stop sign; charge dismissed after he pays a fine and completes a second diversion program.

December 2008 – Applies to enlist in the U.S. Army but is disqualified to serve because of prior drug use.

March 2010 – Asked to leave the animal shelter where he is employed as a dog walker after failing to follow instructions; voices interest in weapons, shooting, and target practice.

January – September 2010 – Engages in disruptive and bizarre behaviors at Pima Community College (PCC), which led to meetings with a school counselor and five contacts with campus police.

August – October 2010 – Posts statements on his MySpace page that indicate he may have been contemplating suicide.

September 23, 2010 - Records and uploads a disturbing video to YouTube about PCC called "Jared Lee Loughner Pima Community College – School Genocide Scam Free Education Broken United States Constitution." In the video, Loughner walks around filming the campus, making bizarre statements such as "This is my genocide school where I'm going to be homeless because of this school" and "This school is illegal according to the U.S. Constitution," and one of the "biggest scams in America."

November 30, 2010 – Loughner purchases a 9mm GLOCK semi-automatic handgun from Sportsman's Warehouse in Tucson, AZ.

November 2010 – Loughner posted a comment online, writing, "I have a new tattoo on my back: 2 9mm bullets," following that with, "There are important figures in my dreams that accomplished political aspirations: Hitler, Hillary Clinton [sic] and Giffords to name a few."

December 6, 2010 – In a search of Loughner's safe post-incident, investigators found a letter from Rep. Giffords's office thanking Loughner for his attendance at the 2007 "Congress on Your Corner Event." In the letter, Loughner had written "Die Cops" and "Die Bitch." Also found in the safe was an envelope, dated December 6, 2010, containing two shell casings on which he had written "I planned ahead," "My assassination," and "Giffords," and words to the effect of "these are the first two shells of my gun." The serial number for a Glock handgun was written on the outside of the envelope.

December 13, 2010 – Posts statements on his MySpace page that threaten law enforcement and suggest he may have been contemplating suicide.

December 24, 2010 – Purchases a 6-inch bladed knife and holster.

Late December 2010 – Visits friends and shows them a gun and bullets.

January 2011 – Researches political assassins and lethal injection on the internet.

January 7, 2011 – Day of the Shooting

- **11:35 PM –** Loughner visited the Walgreens next to the Safeway, where Rep. Giffords's "Congress on Your Corner" event was slated to occur the following morning.

January 8, 2011 – The day of the shooting.

- **12:00 AM –** Shortly after midnight, Loughner checks into a Motel 6.
- **2:00 AM –** Leaves a troubling message on a friend's voicemail.
- **4:12 AM –** Posts "Goodbye… Dear friends" message to his MySpace page.
- **7:04 AM –** Arrives at a Walmart store and attempts to purchase ammunition but is turned away due to his erratic behavior.
- **7:27 AM –** Purchases ammunition and a black backpack-style diaper bag at a Super Walmart.
- **7:30 AM –** Stopped by an Arizona Game and Fish Department officer for running a red light.
- **8:00 AM –** Arrives at his house, where his father questions him about what's in the diaper bag. He mumbles and then escapes his house on foot about twenty-five minutes later.
- **9:00 AM –** Loughner enters a convenience store near his home and asks the clerk to call him a taxi.
- **9:54 AM –** Arrives by taxi at the La Toscana Village strip mall, site of Giffords' "Congress on Your Corner" event, and enters the Safeway with the taxi driver to get change to pay the fare. He then enters the restroom and puts in earplugs.
- **10:00 AM –** Giffords arrives for the event just after 10 a.m. Loughner approaches a volunteer, asks to speak with Rep. Giffords, and is directed to the back of the line.
- **10:10 AM –** Walks back to the front of the line and shoots and injures Giffords. He then turns and fires at the crowd around her, killing six and wounding 13.
- **10:11 AM –** His gun malfunctions and bystanders tackle and hold him down until law enforcement officers arrive.

Those who died:

- U.S. District Judge John Roll, 63.
- Dorwan Stoddard, 76, who was protecting his wife.
- Dorothy Morris, 76.
- Phyllis Schneck, 79.
- Gabe Zimmerman, 30, a social worker and community-outreach director for Giffords' office, who had helped organize the event that morning.
- Christina-Taylor Green, 9, who was visiting the event with a family friend.

May 2011 – Loughner was deemed incompetent to stand trial. As a result, the court ordered a mental health evaluation that diagnosed Loughner with paranoid schizophrenia. He refused to acknowledge that Gifford was still alive as it would make him a "failure." While in jail, Loughner was treated for his mental illness.

November 2012 – He pleaded guilty and was sentenced to life plus 140 years in prison.

Pre-Incident Indicators by Identification Type

Pre-incident indicators resulting from human observation:

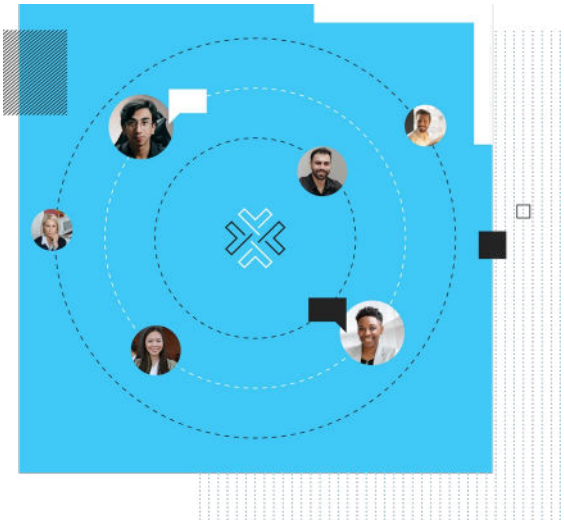
- Exhibited signs of mental illness, such as hearing voices and communicating bizarre ideas.
- Attended the "Congress on your Corner" event with Giffords.
- Verbalized hatred for the government to friends and family.
- Asked to leave the animal shelter where he volunteered for not following instructions.
- Showed guns and bullets to friends.
- Left concerning voicemail for a friend on the day of the shooting.
- Attempted to purchase ammunition from Walmart. After he is turned away, he purchases ammunition from Super Walmart.
- Purchased several weapons: a Heckler and Koch 12-gauge shotgun, Glock 19 semi-automatic 9mm gun, and a 6-inch blade knife. (Source: Department of Homeland Security)
- Application rejected from U.S. Army due to previous drug use. (Source: Department of Homeland Security)

Indicators that technology could have assisted with identifying:

- Posted YouTube videos that were disorganized and disturbing (i.e., Claimed that PCC was a "genocide school").
- Contemplation of suicide via MySpace.
- Posted photos on MySpace of his Glock in the days leading up to the event.
- Posted threatening messages via MySpace towards law enforcement officials.
- Arrested and charged with minor in possession of alcohol.
- Dropped out of high school. (Source: Department of Homeland Security)
- Arrested and charged with misdemeanor possession of drug paraphernalia. (Source: Department of Homeland Security)
- Arrested and charged with vandalism.
- Fired from several jobs.
- Loughner had several interactions with the campus police and other security officers during his time at Pima Community College. In addition, as a result of his concerning behavior on campus, he had meetings with a number of counselors.
- Suspension from Pima Community College.
- Expressed fascination with violence (social media findings, i.e. his tattoo of a 9mm bullet).

Interested in additional reference materials? Check out these articles:

- Security Magazine, Fred Burton: The attack cycle, mass shootings and lone wolves: What companies should know
- Security Info Watch, Manish Mehta: How to implement modern investigations and case management software
- Athletic Business, Fred Burton: As Athletes Play, Bad Actors Can Prey: Why Protective Intelligence is Needed in Sports



About The Ontic Center for Connected Intelligence
The Ontic Center for Connected Intelligence is led by the industry's top thinkers and change makers. They offer invaluable perspectives on present and historical security industry trends while fostering a vibrant community of practitioners. This community comes together to exchange valuable lessons through dynamic discussions, conversations, and alternative analyses.

For more information please visit: ontic.co/center