

Perspectives on Threat Management

Frederick S. Calhoun
Clearwater, Florida

Stephen W. Weston
Pioneer, California

This article describes Calhoun and Weston's blue-collar approach to threat management. It defines seven concepts for an effective threat management program, including identifying hunters versus howlers, situation need to know, situation dynamics and intervention synergy, and ways to avoid bunkers, silos, and myopic management strategies. The article also details 10 guidelines drawn from the authors' experiences managing both hunters and howlers. It looks back over the last 25 years to offer advice to the next generation about the profession's future after achieving professionalization.

Keywords: threat management, threat assessment, hunters and howlers, need to know, situation dynamics

While the Association of Threat Assessment Professionals (ATAP) grew up, we grew older. Along the way, we gained a number of perspectives on what goes into an effective threat management program. We offer here our takes on the following:

- Calhoun & Weston's Blue Collar Approach
- Key Concepts for Effective Threat Management
- Guidelines for Managing Hunters and Howlers
- Back to the Future
- Post-Professionalization

With a combined 50 years working in threat management, we hope that our experiences—and the perspectives derived from them—have something of value to contribute to the field.

Calhoun and Weston's Blue Collar Approach

Over the last quarter century, we strove to offer:

- Practical concepts providing real-life approaches to identifying, assessing, and managing problem individuals;

- Realistic applications that can be easily remembered and readily used;
- Consistent focus on subject behaviors that are noticeable and therefore assessable;
- Real-life situation analyses based on our own and others' actual experiences;
- Hands-on experiences while working real cases;
- Useful tools any practitioner can put into practice immediately.

At the same time, we consciously strove to avoid:

- Theory over practice, always preferring practical over conceptual;
- Generalization over pragmatism, realizing that reality trumps generality;
- Big words;
- Homilies, (with the possible exception of "Hunters hunt and rarely howl; howlers howl and rarely hunt");
- Easy answers, because managing problem individuals should never be considered easy.

We always believed that these approaches, both what we offered and what we shunned, constituted the "blue collar" side of effective threat management; that is, as practitioners and trainers, we never shied from the rough and tumble.

Key Concepts for Effective Threat Management

Over the course of our careers, we stumbled upon a number of notions that seem to us essential ingredients of an effective threat man-

Frederick S. Calhoun, Private Consultant, Clearwater, Florida; Stephen W. Weston, Private Consultant, Pioneer, California.

Correspondence concerning this article should be addressed to Frederick S. Calhoun, or Stephen W. Weston. E-mail: fcalhoun@comcast.net or weston@volcano.net

agement process. They served us well over the years. The most essential of these are the following concepts:

- Hunters and Howlers
- Need to Knows
- Situation Dynamics and Intervention Synergy
- Bunkers, Silos, and Myopic Management Strategies

During any threat management process, the threat manager deals with either a hunter or with a howler. The Need to Knows compose those areas of inquiry that, if all the information were known, would allow for a complete and confident assessment. As the process proceeds, the knowns and unknowns interact with the subject and target generating a constant dynamic. As soon as the threat manager gets involved, intervention synergy further escalates the dynamics. Throughout, the effective threat manager knows to avoid bunkers, silos, and myopic management strategies.

Hunters and Howlers

Problem individuals fall into one of two categories, either hunters or howlers. Over the years, we refined that simple idea by identifying the types of behaviors in which hunters engage and by organizing different types of howlers according to their relationship with, and their intentions toward, their targets. Hunters truly intend to commit an act of violence against whatever target they have selected. They intentionally proceed along what we call “the path to intended violence”; that is, they move from

- feeling a *grievance* to
- *developing the idea* that only violence can resolve their injury, to
- *researching and planning* the attack, to
- *making preparations* according to the dictates of the plan and the opportunities available, to
- *breaching* the target’s security (however primitive or sophisticated that may be), and then to
- *attack*.

Conversely, howlers communicate inappropriately by making threats or improper suggestions or requests, but they never advance beyond those inappropriate communications. The farthest howlers get along the path to intended violence is ideation, but the howler’s idea is to disturb or frighten the target (often multiple targets), not to

cause actual physical injury. The threats may envision death or physical injury, but howlers never advance beyond the vision. Indeed, since howlers rarely see the target’s reaction to the communication, the howler’s imagination fills in the blank, usually with great exaggeration.

Because howlers pose no risk of violence, a threat manager might find it tempting to ignore or brush off the howler’s inappropriate communications. But howlers cannot—and should not—be ignored. Doing so risks potentially dire consequences. Feeling ignored may prompt the howler to escalate his or her behaviors until he or she gets the desired attention. Frequently, too, the howler’s target may demand action, pressuring the threat manager to do something—anything—to make the howler stop. And, finally, howlers are problem individuals because they cause fear. They need managing. Indeed, by all accounts, howlers constitute most of the problem individuals with whom most threat managers deal.

Anatomy of a hunter. On March 10, 1993, Michael Griffen assassinated Dr. David Gunn at the Pensacola abortion clinic where he practiced one day each week. Although Griffen later recanted, within days of the murder Paul Hill established himself as a prime advocate of the unfounded doctrine of “justifiable homicide”; that is, opponents of abortion are justified in killing abortion providers in defense of the unborn fetus. Hill became an instant celebrity. Within a week of Griffen’s shooting, Hill appeared on the *Donahue Show*, read himself quoted in newspapers and magazines across the country, and later appeared on *Nightline* and other news and talk shows. Throughout, Hill claimed that he personally would never murder a provider, but he argued that he believed it entirely justifiable if someone else did.

But no one else accepted his challenge. News organizations turned their attention to other news, other controversies. Hill’s new-found fame diminished, leaving him with his grievous opposition to abortion and his job detailing cars at local car dealerships in Pensacola. Then, on July 21, 1994, Hill moved from grievance to ideation.

In an online essay Hill wrote five years later, he described in his own words how he progressed along the path to intended violence. While cleaning a car and commiserating about the lack of action, Hill (1999, p. 3) remembered:

The idea of acting myself struck; it hit hard. I realized that many people were still reeling from the previous shooting. A second punch, in the same spot, would continue a chain reaction. I began to consider what would happen if I were to shoot an abortionist. My eyes were opened to the enormous impact such shooting in Pensacola would have.

As an active demonstrator outside the Ladies' Center clinic, Hill already knew most of the routines, especially that the doctor visited every Friday. He also knew that his wife planned to take their children on vacation the following week, leaving him alone and thus able to make his plans and preparations unobserved. On Friday, July 14, Hill went to the clinic early where he found another protestor already there. Hill (1999, p. 3) did some research:

After discrete questioning, I learned he had been there when the abortionist had arrived, about 7:30. . . . I discovered that the abortionist had arrived prior to the police security guard. This information was like a bright green light, signaling me on.

Hill's research filled out his plan. He would act the next Friday, with his family safely out of town. Hill (1999, p. 5) described his plan:

My plan was to carry the shotgun from my parked truck to the front of the abortion clinic in a rolled-up poster board protest sign. I would leave the concealed shotgun lying on the ground until the abortionist drove past me into the clinic parking lot.

Now armed with a plan, Hill (1999, p. 5) made some preparations, including practicing shooting at a local gun range and secretly saying goodbye to his family.

One particular obstacle arose to test my determination. While practicing with my shotgun at a nearby gun range, it began to jam. A local sporting goods store had a handy replacement: a 12-gauge Mossberg shotgun with a shortened barrel and an extended magazine. It was called 'The Defender.'

On July 15, Hill (1999, p. 4) took his family to the beach where he played with his children.

They enjoyed their father's attention. I took them one by one . . . in water over their heads as they clung to my neck. As I carried and supported each child in the water, it was as though I was offering them to God as Abraham offered his son.

Friday came and so did the doctor. Hill (1999, p. 6) retrieved his shotgun from the rolled up poster board and began his breach:

God heard my prayers and the abortionist arrived prior to the police guard. . . . When I lifted the shotgun, two

men were sitting in the front seats of the parked truck; Jim Barrett, the escort, was directly between me and the abortionist.

As Hill walked down the driveway, he began firing. He killed the escort first, then walked around to the passenger side and shot the doctor. He remembered (Hill, 1999, p. 6):

When I finished shooting, I laid the shotgun at my feet and walked away with my hands held out at my sides, awaiting arrest.

Hill, like every accomplished hunter, fully intended to commit violence against his target. Fulfilling that commitment took him from grievance to ideation to research and planning to preparation to breach and finally to attack. Over nine years later, the state of Florida executed Paul Hill on September 3, 2003. The day before, prison officials allowed Hill to host a press conference. His advocacy of justifiable homicide ended as it began: on the news.

By identifying a problem individual as a hunter, the effective threat manager can use the steps along the path to intended violence to disrupt the hunter's plans and preparations or to persuade the potential hunter to abandon his or her trek. Such identification also informs the threat assessment and the choice of threat management strategies. Understanding how hunters behave is a key concept in establishing an effective threat management process.

Anatomy of a howler. In 1986, a Maryland court sentenced Scott Rendelman to four and a half months in prison for investing an unsuspecting client's \$283,000 in gold. When the appellate court rejected his appeal, Rendelman sent the court a threatening letter, which got him a 10-year extension on his sentence. He later explained to a reporter:

The first thing that happened was that I lost everything. The credit card people started suing me. The mortgage people came after the house. My wife took the kids and divorced me. . . . And after six months they'd ground me down. I had absolutely no desire to get out. I was ashamed. I didn't want to face my family again, and I had absolutely nothing to go back to. (Wiley, 2002)

Rendelman claimed that someone raped him, thus further robbing his self-esteem. He refused to take a prison job, prompting prison authorities to lock him up "in the hole." He found living there easy.

When I thought about it, I guess I really preferred life in prison. You didn't have to pay bills. They did

laundry for you. Brought you your meals—room service. And I didn't have to show my face and be ashamed. (Wiley, 2002)

In order to stay in the one place where he did not have to feel ashamed, Rendelman began sending other threatening letters whenever he came up for parole or when his sentence neared its end. He threatened President George H.W. Bush and President Bill Clinton, which landed him in federal prison.

The cycle of letter writing and extended prison sentences went on for 15 years. Eventually, he came before a judge who determined “to take Mr. Rendelman finally out of the nightmare he’s been living for the last 15 years.” Rather than sending Rendelman back to prison for the latest threat letters, the judge put him in a half-way house for a year, after which he set him free. Rendelman told a reporter:

That letter writing is over. I just did it from prison basically because I didn't want to be released. Now, though, if they did send me back to prison, that's when I'd start writing again. (Wiley, 2002)

Rendelman returned to Maryland. In 2004, Rendelman sent a letter to the client he had embezzled demanding \$100,000. That and other letters to the client got Rendelman convicted of extortion. As promised, once back in prison his

letter writing resumed. Brought again before a federal court, the judge sentenced Rendelman to 15 years—with no hope of parole. The judge also advised the Federal Bureau of Prisons to closely monitor Rendelman's letters (Castaneda, 2008).

Howlers make a lot of noise, they threaten and extort and try to frighten and disturb their targets. For that reason alone, threat managers must manage them, all the while realizing that they pose little risk of violence unless some event nudges them from howling to hunting.

The Need to Knows

Once the threat manager identifies a problem individual, whether hunter or howler, effective threat management requires gathering information through specific areas of inquiry. We call these areas the Need to Knows and suggest that if enough information is collected from each area, the threat manager can make a fully informed, confident threat assessment about the problem individual. Table 1 presents the 20 Need to Knows.

The Need to Knows are broad areas of inquiry. A quarter century ago, most threat managers asked very specific questions, such as “What did the subject say or write in the inap-

Table 1
Need to Knows

1. How did the subject choose to approach the target?
2. What about the situation indicates the subject's identity and physical proximity to the target; in other words, who and where is the subject?
3. What about the situation indicates who or what the subject is targeting; in other words, who or what is the target?
4. What about the situation indicates the type of venue being targeted and what is it about the venue that gives insight into the subject's intent, motive, and ability?
5. What about the situation indicates whether or not the Intimacy Effect is in play; in other words, what is the nature of the relationship between the subject and the target?
6. What about the situation relates to the subject's choice of context, including the circumstances and content?
7. Is the target currently accessible to the subject?
8. Does the subject have the ability and motivation to take advantage of any current accessibility to the target?
9. Is there a known history of previous contacts with the target or other targets by this subject?
10. Does the subject have a history of violent or threatening behaviors, including any criminal behavior?
11. What is the subject's knowledge about the target's current situation?
12. Is the subject seeking knowledge about the target and the target's current situation?
13. Does the subject's behavior indicate mental health issues, including suicidality?
14. Does the subject possess, have access to, or give evidence of a fascination with weaponry of any type?
15. Is the subject currently seeking to obtain a weapon?
16. What is the status of the subject's inhibitors, including any recent losses?
17. Has the subject exhibited controlling, isolating, or jealous behaviors toward the target?
18. Does the subject have a history of, or is currently, abusing alcohol, drugs, or prescription medicines?
19. Does the subject have any relevant medical issues?
20. Has the subject engaged in any final act behaviors?

propriate communication?" The Need to Knows broaden that question to ask about the subject's choice of context, including the circumstances surrounding the inappropriate contact. The Need to Knows focus the threat manager's attention on the circumstances, the subject's history, and the subject's life circumstances.

Twenty-five years ago, threat managers performed records checks to determine whether the subject owned a firearm. With the Need to Knows, contemporary threat managers focus on weapons possession, but also interest in weapons and violence and any evidence of weapons-seeking behaviors. The Need to Knows also delve into the subject's choice of delivering the inappropriate communication, whether or not the subject revealed his or her identity, whether or not the subject clearly identified the target, the impact of the Intimacy Effect, and the current proximity between the subject and the target.

A quarter of a century ago, threat managers conducted another records check to determine whether the subject had a criminal history. Now, threat managers look for evidence of previous acts of violence, evidence of expressions of using violence, or other behaviors suggesting that the subject used violence to resolve previous problems. Contemporary threat managers ask about the subject's ability and motives, previous contacts between the subject and target, history of violence, and evidence of how much the subject knows about the target, including behaviors seeking knowledge about the target.

Twenty-five years ago, threat managers tried to determine whether the subject had ever been committed to a mental health facility. Today, threat manager's look for evidence of any behavioral health issues (treated or untreated), including suicidality. They ask whether the subject exhibits any delusions, especially involving violent themes. They also ask about any relevant medical issues in general. The Need to Knows focus the threat manager's attention on the subject's life circumstances, including the presence of inhibitors, mental and physical health, substance abuse, and evidence of final act behaviors.

These areas of inquiry both broaden the threat manager's view of the situation and focus the threat manager's attention on issues pertinent to assessing the potential risk of violence. Evi-

dence may not be found for all the areas, thus leaving most assessments incomplete. But what is known can be assessed, even knowing that what remains unknown affects future assessments. And what is known at any given time has to be weighed against the circumstances and context of the current situation.

The weight of each area of inquiry varies according to what is going on at the time of the assessment. For example, evidence of an interest in weapons is of less importance when assessing an avid hunter, but takes on greater weight when assessing someone who only recently evinced such interest during a volatile termination dispute. Context controls the assessment.

Situation Dynamics and Intervention Synergy

Situations requiring threat management are usually marked by great volatility, stress, and extreme sensitivity to changes and new developments. These situations require attention, flexibility, and quick responses. Effective threat management recognizes the volatile nature of problem individuals. The higher the risk, the more combustible the mix.

Situation dynamics. We define situation dynamics as follows:

The evolving interaction between the knowns, the unknowns, and the need to continuously assess each in determining the appropriate protective response at any given point in time.

Keep in mind, of course, that there are two types of unknowns: what is unknown to the threat manager about the subject and what is unknown to the subject about the target, especially any changes prompted by the protective response. The subject certainly knows about his or her own situation. What is generally unknown to the subject is the target and the threat manager's assessment and reaction.

To deal effectively with situation dynamics, the threat manager must first recognize that they exist. That recognition goes a long way toward responding flexibly and adroitly. The threat manager must also recognize that he or she does not control the world. People die, people lose their jobs, couples divorce, accidents happen. All these real-world events can impact a threat management situation at any point in time. This

also requires constant situational awareness in a very fluid environment. All of this may be further upended when intervention synergy comes into play.

Intervention synergy. We define intervention synergy as follows:

The situation dynamic intensified by the stimulus of what the threat manager or target does or does not do in response to the threat situations.

Simply put, intervention synergy means that whatever action or inaction the threat manager takes becomes part of the chemistry of the situation, causing chain reactions. And each reaction prompts new actions. All of this is further confused by the subject's expectations measured against the target's reaction. If the subject expects one outcome and the target reacts differently, then the subject may feel prompted to escalate or try a different tactic.

As with situation dynamics, effective threat management requires the threat manager to recognize the effect of intervention synergy. That requires carefully measuring the impact of any applied threat management strategy, always keeping the synergy in mind. Did the strategy make the situation better, make it worse, or was there no perceptible change? How did the subject react, with an escalation, de-escalation, or a muted response.

The effect of both situation dynamics and intervention synergy demands that the threat manager continuously assesses the situation and be prepared to change strategies if they fail or if they make the situation worse. That is why we say that situations requiring threat management are usually marked by great volatility, stress, and extreme sensitivity to changes and new developments. These situations require attention, flexibility, and quick responses from the threat manager.

Bunkers, Silos, and Myopic Management Strategies

The final group of concepts we believe essential to effective threat management differ from the previous concepts. The previous concepts all pertained to aspects inherent in the threat management process. Problem individuals are either hunters or howlers; a definitive set of areas of inquiry make up the Need to Knows; and every situation generates dynamics and intervention synergy. The

next set of concepts are actions and reactions the threat manager must avoid—and that avoidance is best accomplished by understanding the detrimental aspects of each concept.

Bunkers. The bunker mentality focuses almost exclusively on one side of the situation, thereby blinding security and the target to any additional security risks or threats. Bunker mindsets fall at either end of the security spectrum. Once the physical security countermeasures are in place, those inside the security relax because they feel protected. But security erodes over time, usually because of that feeling of having protection. That complacency blocks anyone from recognizing the degradation of the physical security. But assuming the bunker's security discourages any effort to test it or view it objectively.

Or the bunker mentality can prevent the threat management team from assessing other risks that the subject may pose. The organization may take effective strategies deflecting the subject from the organization. Doing so may inadvertently point the subject toward another unsuspecting target. The management strategies become so concentrated on protecting the bunker that threats to other targets get ignored. By protecting the organization's own bunker, the threat management team releases the subject to look to other targets or on the community at large. By not alerting other security or law enforcement organizations, the bunker mentality endangers other targets while presumably protecting its own. Terminating or expelling a subject from the bunker does not ensure safety.

We have long professed that violence occurs at the edges of security. By that we mean that where security planning ends, a determined hunter's planning begins. Secure the courtroom and the shooting occurs in the hallway. Secure the building and the shooting occurs on the courthouse steps or the parking lot. Provide security for the judge at work and the shooting occurs at his or her residence. This simple truth reveals the weakness in relying on physical security measures and a bunker mentality.

Silos. Information silos have a detrimental effect on information flow regarding threat management cases. The silo effect occurs when internal system components fail to communicate with each other. Imagine a line of silos standing independent of each other, with no means of communication between any two of the silos. The dis-

tance between them thwarts communications and promotes competition among the components. Redundancy creeps in. These adverse effects increase the risk of system failures.

After September 11, law enforcement put in place major enhancements that helped tear down information silos among various agencies related to terrorism at the federal, state, and local level. Unfortunately, significant barriers remain to sharing information due to organizational policies and the sometimes-incomprehensible requirements for top-secret clearances, further compounded by an encapsulating need to know standard. Hypervigilant confidentiality also disrupts information flow concerning personnel matters or legal settlements.

Myopic management strategies. Of all the facets of threat management, the most challenging aspect is the decision of when and how to intervene when a subject exhibits behaviors that potentially pose a threat to an identifiable target. For many reasons, threat managers easily develop myopia when implementing intervention strategies. Knowing that taking any action may worsen the situation, even potentially prompting a violent act, hangs over every threat management decision. Too many threat managers cling to the belief that simply doing nothing offers the best strategy. A poorly reasoned and ineptly executed strategic intervention can be worse than just doing nothing. These concerns, combined with potential targets pressing for action and the inherent difficulties in implementing interventions, can test even the most experienced threat manager.

Imagine a spectrum of situations running from high risk to low risk. At either extreme of this spectrum, the type of response is self-evident. High-risk situations require immediate measures to prevent a violent act. They are emergencies and are easily identified as such. Low risk situations support taking no further action at this time simply because the risk is so benign. The challenge to threat managers lies in the middle of the spectrum, where the situations are not so easily identified as either high or low risk. For most threat managers, most of their time will be spent trying to assess the midrange situations.

The threat manager's training, experience, previous successes, and the organizational environment usually determine the choice of intervention strategies. Threat managers in a law enforcement agency will usually focus on evi-

dence of a crime that can be resolved with an arrest. Corporate security or private consultants working to prevent workplace violence will embrace different strategies for protecting the workplace. Mental health providers tend to rely on mental health strategies.

Ten Guidelines for Managing Hunters and Howlers

Our 50 years combined experience working, teaching, and writing in the field of threat management has left us with a reasonable sense of what works and what does not work in managing problem individuals, whether a hunter or a howler. From that experience, we developed the following 10 simple guidelines threat managers should keep in mind as they manage each type. We purposefully kept them simple because they are so often easy to overlook or forget; yet each guidance composes a crucial element of the threat management process. And, besides, simplicity is part of our blue-collar approach.

1. Be mindful of the context and circumstances in which the subject acts. The first set of Need to Knows—questions 1 through 6—are all areas of inquiry addressing various aspects of the context and circumstances in which the subject came to the threat manager's attention. In threat management, context is everything. Hearing someone threaten the umpire at a contentious baseball game is an entirely different context than an irate husband threatening his wife in the middle of a contentious separation. The threat to the umpire can be dismissed as fan fervor; the intimacy effect invests the threat to the wife with high risk.

2. Always keep in mind the goal of each threat management intervention. Resolving problem situations requires managing the problem person or situation at this moment in time. Each threat management strategy aims to increase the safety of the specific target, other potential targets, and the public at large (including the subject). The strategic intervention must be *proportionate* to the situation and the problem behaviors of the subject; *flexible* enough to handle the situation dynamics and intervention synergy; and *sustainable* over time if the situation requires sustaining. Do not kill a fly with a .45; be prepared to

chase the fly around the room; and keep after the fly until it no longer acts the pest.

3. Make sure to distinguish between hunters and howlers. Hunters engage in attack-related behaviors—they follow the path to intended violence. Howlers engage in inappropriate communications. Each type of problem individual must be managed; neither can be ignored. And remember, too, our one homily: Hunters hunt and rarely howl; howlers howl and rarely hunt.

4. Always gauge the Intimacy Effect, which postulates that the more personal or intimate the relationship between the subject and the target, the greater the value of threats as preincident indicators of violence. Just as importantly, the more impersonal the relationship between the subject and the target, the more likely the value of threats diminishes as a preincident indicator of violence. Threats in the domestic violence venue have very high value. Threats in the public figure venue have very low value. Again, in threat management, context is everything.

5. Be prepared to reassess each situation as events unfold. Threat assessments have very short shelf lives. They are good *at this time*, but not much beyond. Situation dynamics and intervention synergy foster constant changes; those changes need their own assessment to determine their effect on the situation.

6. First, recognize last straw events; second, avoid creating last straw events. A last straw event is something that occurs to the subject that prompts him or her to step out on the path to intended violence. For Paul Hill, his last straw was realizing that no one had taken up his call for justifiable homicide and that the absence of such action had diminished his celebrity status. Like the grievances that spawn last straw events, the last straw is unique to each hunter, thereby making recognizing them admittedly difficult. But that also makes avoiding creating a last straw event fairly straightforward.

7. Approach problem situations flexibly and innovatively. Problem situations are fluid, with new events occurring near constantly. That fluidity and novelty can only be matched with flexible and innovative responses based on continuous reassessments as the situation evolves. Effective threat management is

not, we assure you, an endless process; it just seems like one.

8. Always keep the “dignity domino” propped up. The most important inhibitor keeping problem individuals from pursuing the path to intended violence is the subject’s sense of personal dignity. Once that topples, most individuals feel they have nothing left to lose. They may even feel that acting violently restores their self-worth. Oftentimes, hunters wrap their violent act in a cloak of grandiosity. On August 26, 2015, Vester Flanagan II brutally killed a TV reporter and her cameraman while they were on the air. Flanagan justified the shooting as an attack on racism prompted by the slaughter of nine Blacks at a Charleston, SC church by an admitted racist. In reality, Flanagan had been fired from the TV station years before and he never recovered his sense of importance. He went from perceiving himself as an on-air TV celebrity to working as a receptionist at Risk Management Programs, Inc., a temp worker whom full-time colleagues found unimpressive. Most of Flanagan’s complaints focused on how people treated him, all insults and injuries (Shear & Nir, 2015). Under these conditions, Flanagan’s dignity domino toppled.

9. Stick to the facts and avoid the “What If?” Game while hoping for the best, but planning for the worst. The “What If?” Game occurs when the threat manager begins imagining all the terrible things the subject could be up to at this very moment. The threat manager has no evidence to support such imaginings, but because the things are so terrible the threat manager feels they cannot be ignored. In fact, they should be ignored and the facts—and only the facts—should alone be assessed. Based on a factual assessment, appropriate protective responses can be erected, always with the idea that we hope they work, but having backup plans if they do not.

10. Manage problem situations for as long as they need managing. Problem situations do not go away just because the threat manager and the target wish them away. They can only be resolved through effective threat management, no matter how long it takes to work. And problem situations end only after a factual reassessment determines that the subject does not pose a risk to the target at this time.

Calhoun and Weston Back to the Future

Commemorating ATAP's silver anniversary prompted us to reflect on what advice we would give our younger selves if we could hop into our suped up DeLorean and go back two and a half decades. Although skeptical that our younger selves would have listened to any advice from two over-the-hill seniors, the advice does reflect our mature musings.

First, we would advise our two beginners to listen to everyone across venues and specializations because no one has the golden ticket to knowledge, especially in the budding field of threat management. We would then encourage the duo to foster collaboration, not competition, with others in the emerging profession. Indeed, to this day, the profession continues to need active collaboration to ward off some of the disturbing signs of active competition.

Third, we would urge the younger Calhoun and Weston to get some experience in the real world and not to draw solely from research and academic studies. Research has its place, of course, but nothing replaces hard-earned experience actually interviewing angry subjects, communicating with the mentally ill, and actually managing situations. From there, we would caution our younger selves to periodically recognize their gaps in knowledge and experience and to work hard filling those gaps in. Self-reflection staves off self-importance.

Fifth, our younger selves should operationalize the theories, academic studies, and emerging concepts to make them practical in the real world. It is one thing to study and understand the Intimacy Effect, we would tell ourselves, but quite another to use its impact in an actual threat assessment. Next, we would admonish the two to act smarter, not tougher. Threat management is not about scaring off the subject; it is about crafting intelligent, effective responses to complicated, potentially dangerous situations.

Seventh, we would caution our youthful selves to always keep in mind the big picture. That goal is to keep everyone safe, not just the specific target at the moment. Finally, we would urge the younger Calhoun and Weston to become educators and mentors for those just entering the profession afresh. Experience dies with the one who experienced it unless the expert takes the time and makes the effort to

pass it along to the next generation. Let's hope that generation listens to this sage advice.

Post-Professionalization

Over the course of the last 25 years, the field of threat management fully matured into the threat management profession. It now has all the hallmarks of any profession:

- Systematic theory of its own
- Recognized authorities
- Ethical code of conduct
- Specialized vocabulary
- Training and certification.

These are the requisite elements of any profession.

But what next? We see a number of challenges confronting the profession in the years just ahead. We know the questions that must be addressed as the profession moves forward, even if the answers seem to lie just out of reach.

- Should organizations requiring expertise in threat management rely on in-house experts versus outside consultants?
- Should threat management be a full-time assignment or an as-needed assignment?
- Is threat management, entailing as it does the risk of violence, becoming a government function or a private business responsibility?
- Should regional, multidisciplinary, public or private working groups be maximized?
- Is threat management a place for generalists or specialists?

How we as a profession address these issues will determine the future direction of the post-professionalization era of threat management.

We have always believed that predictions are the province of angels and fools, so we admit to playing fools (we're no angels) in making the following prediction concerning how we see the profession evolving. Over the last quarter century, a general understanding of how threat management works effectively developed. The field put threats into the context of the Intimacy Effect and the path to intended violence highlighted the types of behaviors violent individuals engaged in. Research on school shootings uncovered the phenomenon of "leakage," which undoubtedly also occurs in other settings, such as workplaces and gathering places.

Having reached a general understanding and consensus on effective threat management, we

foresee an upcoming venue specialization. The general understanding is like getting a B.A. or B.S. in threat management. The Masters and Ph.D. level are the specializations in whatever venue the practitioner practices. Without question, significant differences are emerging from each of the various venues where intended violence occurs. The most obvious difference is the value of threats as preincident indicators of violence in the public figure venue compared to the domestic violence venue. Effective threat management requires embracing the unique features of each venue and incorporating them into the threat management process. But we feel no confidence that all of the unique attributes have been identified for each venue. That, we think, offers the most fruitful area for future research.

Hence, we believe that before too long we will have practitioners with threat management Masters and Ph.D.'s in the following venue specializations:

- Public figure violence
- Domestic violence
- Workplace violence
- Gathering place violence
- Representative or symbolic violence

The B.A. general understanding will always be a prerequisite, but we foresee venue specialization as we learn more and more about how the different venues actually differ. We believe that future generations of threat managers

- Will have an overall understanding of intended violence across all venues
- With a specialized understanding of intended violence within their venue.

If that happens, we would also hope that the various specialists will share their experiences with other specialists to better inform the gen-

eralist education. Failing to do so would fragment the field.

And to end on a word of caution, we identified several pitfalls to avoid, including:

- Losing a healthy balance between academic theory and practical approaches;
- Losing a healthy balance among subject matter experts—Mental health professionals, Law Enforcement, and Security Consultants; and
- Competition overcoming collaboration.

With diligence and discipline, these traps will be easily avoided.

We envision the threat management profession evolving and improving. Undoubtedly, new concepts and new approaches will continue to emerge, building on the experiences of the last quarter century. The future of the profession appears to us very bright indeed. And the Calhoun and Weston who grew older as ATAP grew up look back on an amazing ride. We take great pride in our small part of that journey.

References

- Castaneda, R. (2008, April 22). Man gets 15 years for threat letters. *The Washington Post*. Retrieved from <http://www.washingtonpost.com>
- Hill, P. (1999, June). Why I shot an abortionist (pp. 1–6). Retrieved in 1999, from www.armyofgod.com/PaulHillindex.html (copy available from the authors).
- Shear, M. D., & Nir, S. M. (2015, August 27). A life of listing grievances, and then Virginia gunman's final homicidal explosion. *The New York Times*. Retrieved from <http://www.nytimes.com>
- Wiley, W. (2002, February 15). Threatening letters turned short term into 15 years. *The Sacramento Bee*. Retrieved from <http://www.sacbee.com>