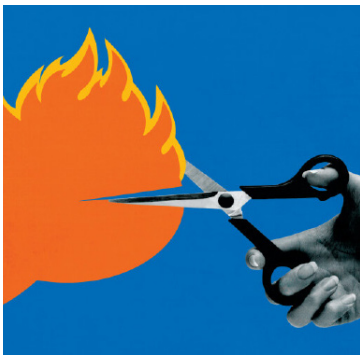
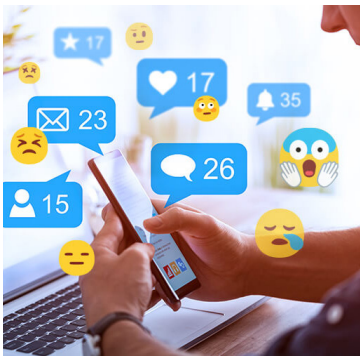
SECURITY MANAGEMENT

Powered by ASIS INTERNATIONAL Advancing Security Worldwide®

Mainstreamed Extremism in the Workplace

This collection of articles from the security profession's premier publication takes a look at extremism, risk, and mitigation.





SECURITY
MANAGEMENT

Combating Complacency: Lessons Learned from the 1994 AMIA Bombing in Argentina

World events from 9/11 to today demonstrate that violence and extremism are a prevalent threat, with the risk of right-wing terrorism rising globally. But 25 years after a major terrorist attack in Argentina, complacency is setting in.

With more than 200,000 members, the Jewish community in Argentina is the largest in Latin America, and the sixth largest in the world; only Canada, France, Israel, the United Kingdom, and the United States have larger Jewish populations. Buenos Aires City, Argentina's capital, is home to more than 200 sites dedicated to Jewish life, including synagogues, schools, yeshivas, and sports centers.

The Jewish people first came to Argentina from Russia, escaping famine and anti-Semitism in the 19th century. In the 1930s, they came to escape a hostile Europe. Following the Holocaust, they fled from horror and

looked to Argentina for a new horizon. While Argentina provided a safe harbor, it was not without threats, especially as the years went by.

At 9:53 a.m. on 18 July 1994, a truck bomb exploded at the AMIA building, killing 85 people, injuring hundreds, and destroying the building. AMIA is a central Jewish institution, responsible for managing cemeteries, coordinating Jewish education, and overseeing a job bank. It sits in the center of the neighborhood known as Once, a traditional Jewish area that is home to kosher sites,

To this day, not a single person is in prison for this horrific crime.

synagogues, schools, and many Jewish-owned shops.

The 1994 attack was not the first to affect the Jewish people of Argentina. Two years prior, in March 1992, a car bombing at the Israeli Embassy in Buenos Aires killed 29 people.

Those were painful and sad times. The Jewish community was not the same. Parents feared sending their children to school and to youth centers. Buildings were not prepared to hold activities in a safe manner. Security personnel was not available to guard institutions. The Argentine State was not prepared to assist.

The security organization of the Jewish community had to rethink everything.

The Jewish representative institutions created a Central Security Office to assess every aspect of community security. Each building was analyzed and hardened. Jewish institutions implemented standoff means, first through cement-filled barrels and later through more

permanent reinforced concrete bollards. Each facility incorporated a security chief and guards, all Jewish. The Central Office was in charge of vetting, recruiting, training, and auditing personnel and activities.

Volunteers from the community guarded events and synagogues when professional security was not available.

Cameras, walls, fences, mantrap doors, and bullet-proof glass were installed, and security procedures were implemented among the different schools, social clubs, and synagogues.

In time, the police started guarding Jewish buildings around the clock.

The Jewish community in Buenos Aires then developed a Community Emergency Plan. The plan assessed the main threats to Jewish life and established the response efforts to each of those, the impact on all institutions, the role of professional security personnel, the role of volunteers, the emergency security operation center's (SOC) mission, and the creation of a backup SOC outside of the central Jewish security building.

A remembrance event is held every year for the 1994 attacks. Several thousand people gather and say the names of the dead. Community leaders, friends, and family of the deceased ask for justice. To this day, not a single person is in prison for this horrific crime.

The remembrance event is held at the new AMIA, rebuilt on the same site as the previous one, with modern and robust security. The events themselves are considered targets, and they are scrupulously protected.

I was a volunteer for the Jewish Security Organization for 16 years, and I have worked professionally in Jewish security as an auditor, instructor, and executive director of the security organization. I worked in the new AMIA building for seven years, spending my time with people

who survived for days under the wreckage in the aftermath of the attack.

When I talk to people from the Jewish community who were born after the attack, their memories of the event and what came afterward are weak. Weaker still are the memories of those who are not Jewish. Argentinean society is forgetting. Its memory is fading. And so is its vigilance.

Each year, less and less budget is designated to security for the Jewish community. The Central Office has reduced its staff and activity during the last five years,

The lack of expertise in terrorism phenomena is a voiced secret.

impacting the services and products provided to security professionals. Training has also been reduced.

The emergency plan has also suffered; updates and drills are less common. Most Jewish institutions face economic constrains and have reduced security personnel and coverage. This affects the capacity to implement proper controls, which when added to the willingness of organizations to be more welcoming to outsiders, affects the stringency of screenings and controls for visits and vendors.

Increasing urban security challenges mean police personnel are no longer at fixed locations like synagogues. They patrol the area instead. This shows the neighborhood that police protect everybody, but the adjusted security posture lifts some protections for Jewish sites.

World events from 9/11 to today demonstrate that violence and extremism are a prevalent threat, with the

risk of right-wing terrorism rising globally. But in Argentina, people are starting to drop their guard. Security is no longer a priority, and attention is scarce.

In the intelligence community, the lack of expertise in terrorism phenomena is a voiced secret.

Civil unrest grows worldwide, the uncertain effects of the COVID-19 pandemic loom, and the conflict between Israel and Hamas has translated into demonstrations in Argentina. Palestinian organizations and left-wing parties recently rallied in front of the Israeli Embassy building in Buenos Aires.

During the early days of the Israeli–Hamas conflict in May 2021, anti-Semitic graffiti was sprayed on a Jewish school in the city of Bahia Blanca in Argentina; it read: "Jewish Rats—We are going to kill you," Argentine news platform *Infobae* reported.

Anti-Israel graffiti sprayed on a traditional Jewish neighborhood of Villa Crespo in the city of Buenos Aires by a right-wing nationalist group read: "Israel intruder" and "Israel genocide," according to *Infobae*. On the street center of the province of San Juan, another graffiti read "Be a patriot, Kill a Jew"—a traditional war cry by traditional right-wing anti-Semitic groups in the 1970s.

Anti-Semitic attacks repeat all over the country. In April 2021, the FBI and the Argentine Federal Police arrested several men charged for an alleged connection to ISIS. One of the people under investigation said that he had instructions for assembling explosive devices, according to *LA NACION*.

Also in April, in the Province of Tucumán, two men were arrested after Argentine police determined that an attack against a synagogue was imminent. During the investigation, authorities seized several firearms and knives, in addition to Nazi literature and symbology.

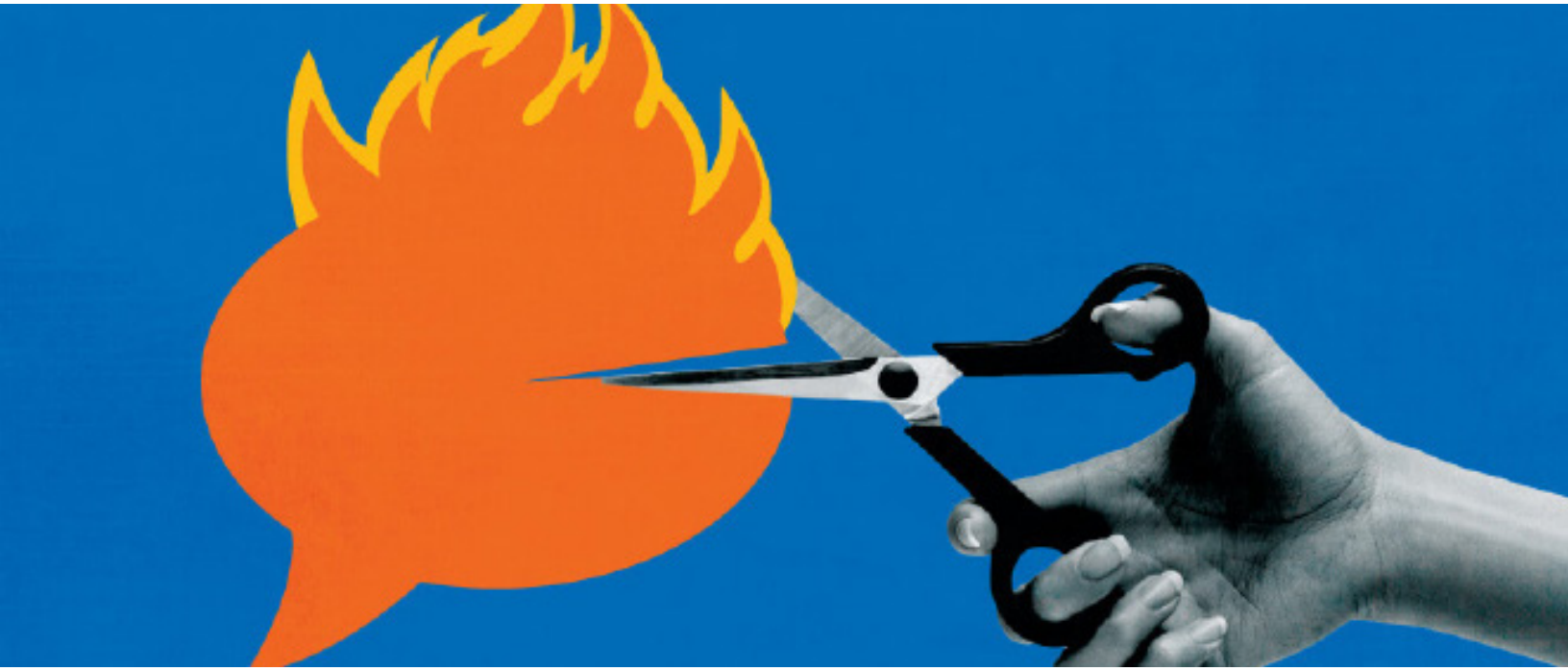
As the time since the last severe attack grows, we are normalizing a reality that nothing tragic happens. Until it happens again.

ALEJANDRO LIBERMAN, CPP, IS A SECURITY PROFESSIONAL AND ASIS MEMBER WITH ALMOST 20 YEARS OF EXPERIENCE. LIBERMAN OWNS CONSULTING COMPANY GLOHER GROUP, LEADING SECURITY CONSULTING, TRAINING, AND INVESTIGATIONS IN SOUTH AMERICA. FROM 2008 TO 2012, LIBERMAN WAS THE HEAD OF THE JEWISH SECURITY OFFICE IN ARGENTINA AND HAS BEEN INVOLVED IN JEWISH COMMUNITY SECURITY FOR 15 YEARS. HE IS ADVISOR TO THE LATIN AMERICAN JEWISH CONGRESS ON SECURITY, CRISIS MANAGEMENT, AND TERRORISM. LIBERMAN SERVED AS THE PRESIDENT OF THE BUENOS AIRES, ARGENTINA, ASIS CHAPTER IN 2020 AND 2021.

SECURITY
MANAGEMENT

The Insider Threat and Extremist Rhetoric

The traditional approaches to mitigating insider threat risks may be effective in reducing the incendiary quality of extremist rhetoric before it results in harm or destruction.



The frequency of malicious insider threat incidents is on the rise—spiking by 47 percent between 2018 and 2020, according to the Ponemon Institute's *2020 Cost of Insider Threats: Global Report*. This growth has roughly coincided with the expansion of media transmissions of opinions and viewpoints from activists on both the right and the left, some of which may be appropriately described as extremist.

While the growth of polarizing and extremist rhetoric may be most commonly attributed to an advancing Internet, the traditional approaches to mitigating insider threat risks may also be effective in reducing the incen-

diary quality of extremist rhetoric before it results in harm or destruction.

American cybersecurity software company Code42 recently noted that the COVID-19 workplace environment has increased the presence of insider threats. The study, conducted by the Ponemon Institute, found that:

"Both business and security leaders are allowing massive insider risk problems to fester in the aftermath of the significant shift to remote work in the past year. During that same time, three-quarters (76 percent) of IT security leaders said that their organizations have experienced one or more data breaches involving the loss of sensitive files and 59 percent said insider threat will increase in the next two years primarily due to users having access to files they shouldn't, employees' preference to work the way they want regardless of security protocols and the continuation of remote work. Despite these forces, more than half (54 percent) still don't have a plan to respond to insider risks."

Indicators of potential insider threat are drawn typically from the following categories: access attributes; career and performance records; foreign considerations; security and compliance incidents; technical or network activity; criminal, violent, or abusive conduct; financial considerations; substance abuse and addictive behaviors; and judgment, character, and psychological considerations.

A sincere and responsible effort to appraise a suspected insider threat leads to a number of particularly insightful questions. Does the individual demonstrate declining performance ratings? Have there been Human Resources complaints? Has there been a reprimand? Does the individual possess a high level of clearance? Does the individual engage in frequent foreign personal travel and

fail to report foreign personal contacts? Have there been security violations or reports of working at off-hours? Has the individual violated information systems policies or introduced unauthorized software? Have there been signs of unexplained affluence? Has there been criminal violent behavior, weapon mishandling, signs of substance abuse or drug test failure, falsifying data in the workplace, or expression of extreme despair?

According to the National Insider Threat Task Force Mission Fact Sheet, a single indicator may say little. If taken in conjunction with other indicators, however, a pattern of concerning behavior may arise that can add up to someone who could pose a threat.

A sincere and responsible effort to appraise a suspected insider threat leads to a number of particularly insightful questions.

The fact sheet further notes:

> "It is critically important to recognize that an individual may have no malicious intent, but is in need of help. We have invested a tremendous amount in our national security workforce, and it is in everyone's interest to help someone who may feel he or she has no other option than to commit an egregious act—such as espionage, unauthorized disclosure, suicide, workplace violence, or sabotage. Intervention prior to the act can save an employee's career, save lives, and protect national

security information. There are also unwitting insiders who can be exploited by others."

This process ultimately yields a personal profile of a suspected insider threat that allows for correction, as well a possible prosecution. The U.S. Department of State's Insider Threat Program works to deter, detect, and mitigate insider threats to protect its organization's people, facilities, information, and reputation, according to "Building a Culture of Trust" from *State Magazine*. The program strives to build a culture of trust and organizational wellness and emphasizes the aim of "turning a suspect around" rather than "turning a suspect in."

The program's officers make available an extensive array of educational tools, including briefs, articles, charts, videos, and online and in-person training exercises, which, in addition to training, may also serve to establish a reassuring and congenial relationship with employees who participate. Responses to reports of suspected insider threats—such as extremist rhetoric—are formed on a case-by-case basis.

JAMES T. DUNNE, CPP, IS A MEMBER OF THE ASIS COMMUNITIES FOR EXTREMISM AND POLITICAL INSTABILITY AND INFORMATION TECHNOLOGY SECURITY. HE IS A SENIOR ANALYST IN THE STATE DEPARTMENT'S BUREAU OF DIPLOMATIC SECURITY.

THE VIEWS EXPRESSED HERE ARE THOSE OF THE AUTHOR, AND DO NOT NECESSARILY REFLECT THOSE OF THE U.S. DEPARTMENT OF STATE OR THE U.S. GOVERNMENT.

SECURITY MANAGEMENT

Extremism in Plain Sight: Recognizing and Responding to Symbols and Threats

We live in a world filled with visual images, and their meanings often changed based on context. So what does this mean for monitoring signs of extremism in the workplace?

What happens when evocative images make their way into the workplace? On our desks, notebooks, clothing, behind us on Zoom meetings, or on car bumpers—what does this mean for organizations? It has the potential to result in increased tensions, conflict, and even the identification of a member of an extremist organization. How does this impact the reputation of an organization or the working environment?

The prospect of responding can seem daunting, but inaction or the wrong action can be as damaging as the image itself. Using the COPE framework to help inform your policy in this area can help. According to Diana

Concannon and Michael Center in "Security in Context" (*Security Management*, August 2020), the COPE framework is a simple model that applies "contextual intelligence to enhance decision making at the executive and managerial levels and on the front lines."

We live in a world filled with visual images. According to recent research, images are central to how we interpret things, give meaning, and communicate with others. Our ability to absorb and interpret visual in-

The meaning derived from a visual, however, is as much about the context in which we see it as it is about the image itself.

formation is the basis of the industrial society and the information age. The meaning derived from a visual, however, is as much about the context in which we see it as it is about the image itself. Once it is removed from this context (which now is easier because of powerful editing technology) and placed within another, it can have a multiplicity of possible new meanings, found researchers in a 2017 report, *Critical Studies on Terrorism*. Even the most definitive, universal symbol can be disconnected from its traditional meaning and appropriated for another cause.

"The meaning derived from a visual, however, is as much about the context in which we see it as it is about the image itself."

So, what does this mean for monitoring signs of extremism in the workplace? If the meaning is not fixed, could a symbol often associated with an extremist group be entirely innocent in another context?

The answer may be yes, given that even one of the most contentious symbols, the swastika, had a peaceful association prior to being co-opted by Nazis in the 1920s. The laurel or olive branch is another case in point and highly relevant today given that it is becoming increasingly synonymous with far-right groups. Groups such as the Proud Boys, Sons of Odin, the Atomwaffen Division, and the Aryan First use it in their symbols and or logos. The appropriation of the symbol by these and similar groups is likely linked to the use of laurel by the Nazis. As Cynthia Miller-Idriss notes in her book *The Extreme Gone Mainstream: Commercialization and Far-Right Youth Culture in Germany:*

"The brand Fred Perry, for example, has a long history of being used by far-right youth because of its logo—a wreath of laurel branches—evokes military insignia used by the [National Socialist German Workers' Party] NSDAP. On some Fred Perry polo shirts, moreover, the collar has black, red, and white stripes—colours that… are popular with far-right youth for their historical significance with national movements and regimes in Germany, including the Nazis."

The use of the laurel in a logo or symbol is not inherently racist, as the symbol is commonly used by extremist groups of a variety of political and religious persuasions. Groups like the al-Aqsa Foundation, Eela Padai (a unit or branch of the Liberation Tigers of Tamil Eelam or LTTE), Mujahadeen-e-Khalq Organization (MEK), People's Liberation Army (PLA) in India, and the Ulster Freedom Fighters have all used it in their logos, according to *Branding Terror: The Logotypes and Iconography of Insurgent Groups and Terrorist Organizations*. This serves to illustrate that diverse groups often use similar symbols, despite significantly divergent ideologies or beliefs.

We should not forget that other groups also use laurel and olive branches in their symbols; for example, the United Nations uses a laurel wreath in their logo, as does Mercedes-Benz. You can probably think of many more.

Given the range of contexts in which a similar image can be used, how (or even can) organizations identify symbols or images within the workplace that might indicate an extremist threat? Is this even the question we should ask, especially given that symbols can be appropriated with significant ease (as evident in memes and the like)? Should we not be asking more nuanced questions that seek to better understand how an organization can equip its staff to have a conversation about signs, symbols, and images that employees see within an organization and may be concerned about? These skills could also be applied to other contentious issues.

The COPE framework provides an effective approach to help us do this, and to help inform the type and nature of the questions we should ask about the potential role of the visual within our organizations, as well as the responses we take. Its merits are multiple, but chief amongst them is the shared understanding of context, which makes information meaningful. Second, it is a simple but powerful framework that allows us to apply contextual intelligence to enhance decision making. Third, the four key elements of the framework— culture, organizational values, politics, and environment—all significantly influence how meaning is derived from an image.

The culture in which we are raised—our reference points—often influences the meaning we derive from images. Similarly, culture also often influences the type of images used by extremist groups. For example, popular conceptions of ancient Norse culture significantly influence the far right.

"The four key elements of the framework— culture, organizational values, politics, and environment—all significantly influence how meaning is derived from an image."

The COPE framework applies in the context of the visual as it allows organizations or employees to react, while also ensuring they check any cultural biases that may affect their response to an image, for example. Organizations should do this to move beyond declaring workplaces as apolitical, while also claiming to promote diversity. Promoting diversity needs to come with an opportunity for peer learning, understanding, discussion, and mediation.

The four key elements of the framework— culture, organizational values, politics, and environment— all significantly influence how meaning is derived from an image.

Using a framework such as COPE allows an organization to show they are taking active measures to both value and support diversity, manage differences, and accommodate different points of view. Adhering to this process can help organizations and employees learn about why certain images are important for some and evocative for others. This helps with peer learning, and in creating an environment that seeks to understand, rather than to close off conversation.

For example, a hypothetical multinational firm marks an employee's first day with the company by asking them to introduce themselves to their colleagues through four images. The experience in the past had caused laughter, tears, and often healthy rivalry be-

tween competing sports fans. The exercise was a good icebreaker for new staff.

Today is Mary's first day. Having thought about it for a while, she presents a picture of her family; one of her garden (she is a keen gardener); one of her graduation (she was the first in her family to graduate from university); and one of her grandmother holding a rug, a family heirloom (to illustrate her family's Navajo origins).

As the fourth image goes up on the screen, murmurs can be heard in the room. A colleague stands up and says that they find the image offensive, and tensions begin to rise. Mary is dejected—how could an image of a rug, one she is so proud of, cause so much offense? This was part of who she was, her history, her culture.

An image of what Mary recognized as a traditional Navajo whirling log pattern on the rug, however, was viewed as a swastika by others. Mary had not thought of the symbol as a swastika when she looked at the rug, yet it was the only thing that the others saw.

So what do you do next?

Consider having a conversation with those offended and Mary, and promote a willingness to be part of a conversation to encourage peer learning and understanding.

Acknowledge from the outset that the conversation may be difficult and set ground rules to encourage the sharing of opinions, knowledge, and hurt.

Ask others within the wider company, who may have remained silent during the presentation, to be part of the conversation.

Prepare for the exercise by conducting prior research and select someone to facilitate the conversation constructively. Mediate where necessary, and consider culture, organizational values, politics, and environment.

Encourage a willingness to listen, ask questions, learn, and share.

Debrief after each event—get the whole group to provide feedback and make changes to this reconciliation process for the next time. This process can be applied to a range of other topics that might cause in-group tensions.

Always remember the shared goal is to make the workplace more inclusive, diverse, supportive, and resilient.

There is no right way to interpret an image. Their meanings can be fluid, and therefore an organisation needs to ensure any policy taken to respond to visual hate or extremism is flexible; even better if such policies can support open and honest dialogue and curiosity, which promotes diversity, inclusion, and respect.

SHEELAGH BRADY HAS MORE THAN 20 YEARS OF EXPERIENCE IN POLICING AND SECURITY. SHE BEGAN HER CAREER IN AN GARDA SIOCHANA, THE IRISH POLICE FORCE, AND THEN MOVED TO THE INTERNATIONAL SECURITY ARENA, HOLDING POSITIONS AS A MISSION SECURITY ANALYST WITH THE EUROPEAN UNION BORDER ASSISTANCE MISSION IN LIBYA, SENIOR SECURITY INFORMATION ANALYST, WITH UNDSS IN ABUJA, NIGERIA, AND ANALYST WITH THE EUROPEAN UNION POLICE MISSION IN BOSNIA HERZEGOVINA (BIH). SINCE 2014, SHE HAS PROVIDED SECURITY RELATED RESEARCH AND RISK MANAGEMENT CONSULTANCY SERVICES FOR INTERNATIONAL ORGANIZATIONS AND CORPORATIONS IN FIELDS SUCH AS ORGANIZED CRIME, TERRORISM, AND CORRUPTION. SHE IS CURRENTLY UNDERTAKING A PHD AT DUBLIN CITY UNIVERSITY (DCU).

SECURITY MANAGEMENT

Balancing Tolerance of Diverse Views and Workplace Violence Prevention: When Extreme Views Lead to Extreme Acts

Left unchecked, extreme beliefs can not only threaten cohesion and productivity, they can compromise safety and raise the risk of disruptive behaviors, even violence.

The contemporary organization strives for inclusion and diversity—not simply in terms of demographics, but in attitudes, opinions, and ways of thinking. Diverse ideas can fuel innovation and create radical change, leading to new levels of success. While diversity can strengthen an organization, strong or extreme beliefs in the workplace can be a two-edged sword. An employee's passion for a belief or cause might manifest itself as a real commitment to their employer or a project, but it can also create friction, erode workforce cohesion, and consume valuable resources when dealing with conflict.

Finding the right balance between welcoming diverse views and minimizing tension between those who hold those views and others can be tricky, but it is necessary. Left unchecked, extreme beliefs can not only threaten cohesion and productivity, they can compromise safety and raise the risk of disruptive behaviors, even violence.

A challenge for those tasked with workplace safety and security is recognizing when beliefs and behaviors begin to approach a red line—when they are not simply strong feelings, but potential pre-incident indicators of risk or possible signs or symptoms of mental illness. Strong beliefs, extreme beliefs, and conspiracy theories are often tinged with a sense of grievance—the thought that something is wrong and there is someone to blame. In the threat assessment field, grievance is recognized as an entry point to the pathway to violence.

Extreme beliefs and conspiracy theories often develop around the idea that a person, group of people, or way of life is under threat by dark forces within an organization, community, or culture. Paranoia about the perceived threat leads to defensiveness and an us-versus-them mentality. It can create the sense that a person or group is at war with others around them who do not subscribe to the same ideas—the nonbelievers.

Paranoia is an established risk indicator for workplace violence; that is not news. Employees who are convinced that their coworkers, supervisors, or organization present an imminent risk may act preemptively to protect themselves or others they believe are in danger. Many instances of workplace violence have been inspired by paranoia. Someone who is paranoid harbors excessive distrusts without justification and may believe that sinister plots are swirling around them. Sometimes paranoid people feel compelled to use violence to stop a real or perceived threat.

Extreme thoughts can become extreme actions.

In a workplace culture that promotes inclusion and diversity—not just who people are, but how they think—how does the organization recognize and tolerate deeply held, sometimes extreme beliefs? What are the thresholds for speech and conduct in the workplace, and how should the organization respond when someone approaches or crosses the line between extreme ideas and extreme behaviors? These are important questions for leaders at all levels in an organization, but especially pressing for security, legal, and HR professionals.

Extreme thoughts can become extreme actions.

When speech and conduct are perceived as disruptive or potentially dangerous, it is important that they be viewed as potential risk indicators and never simply brushed aside. While it is important to create a workplace culture that tolerates diverse, powerful, and sometimes unpopular attitudes or beliefs, it is never acceptable to say, "Oh, that's just that employee being themselves—it's just who they are or how they are." The failure to recognize and respond to hostile communications and behavior leaves open the possibility of escalation.

An employee who subscribes to the QAnon ideology, for example, might deeply believe that liberal elites and other actors in an imagined "deep state" are working to cover up child sex trafficking operations by forcing the pubic onto the 5G cellular network where they can manipulate communications about their nefarious activity that might expose them. That may seem like a pretty far-fetched belief, and it certainly may raise some eyebrows around

the water cooler, but if that same employee now is refusing to communicate with coworkers who have 5G phones, there may be a direct and immediate impact on productivity and team cohesion in the workplace. This sort of disruptive behavior crosses the line between free speech into behavior with real world consequences.

U.S. Department of Justice and FBI research suggests that individuals who commit mass violence in a workplace, school, or community typically exhibit four to five observable indicators in the lead up to their attacks. Violent action is often proceeded by hostile rhetoric. Ideas that are associated with an extremist movement

Ideas that are associated with an extremist movement and represented by hateful language, images, or actions cannot be left unchecked.

and represented by hateful language, images, or actions cannot be left unchecked. In most instances an organization's code of conduct for employees will address hateful speech or actions, and it will clearly communicate the potential consequences for such behavior. But organizations cannot regulate what people think or believe.

In approaching an individual who holds extreme attitudes or opinions that have become disruptive or concerning, it is important to focus on the behavior, not the belief. Trying to convince someone that their worldview is incorrect or delusional is a fool's errand. Such individuals often push back citing their rights to free speech or other legal rights. Attempts to intervene, de-escalate conflicts that may arise from extreme beliefs, or to conduct thorough risk of violence assessments must be focused on the facts—specifically the communication or behavior of concern.

Depending on the nature and seriousness of the employee's belief, it might be advisable to meet with the individual to further assess the quality and strength of their beliefs and to review how discussion of the extreme ideas in the workplace affects other employees or the work environment. The *ASIS Standard on Workplace Violence and Active Assailant* suggests the use of outside consultants in complicated cases where specialized knowledge or skills are required to determine the level of concern.

Research in this area makes it clear that even highly qualified and credentialed forensic psychiatrists and psychologists may have difficulty distinguishing between extreme belief and delusions. At present, there are no clear best practices in managing extreme beliefs in the workplace, and each situation will likely need to be addressed on a case-by-case basis working within the existing frameworks of security, human resources, legal, and threat assessment policies and procedures.

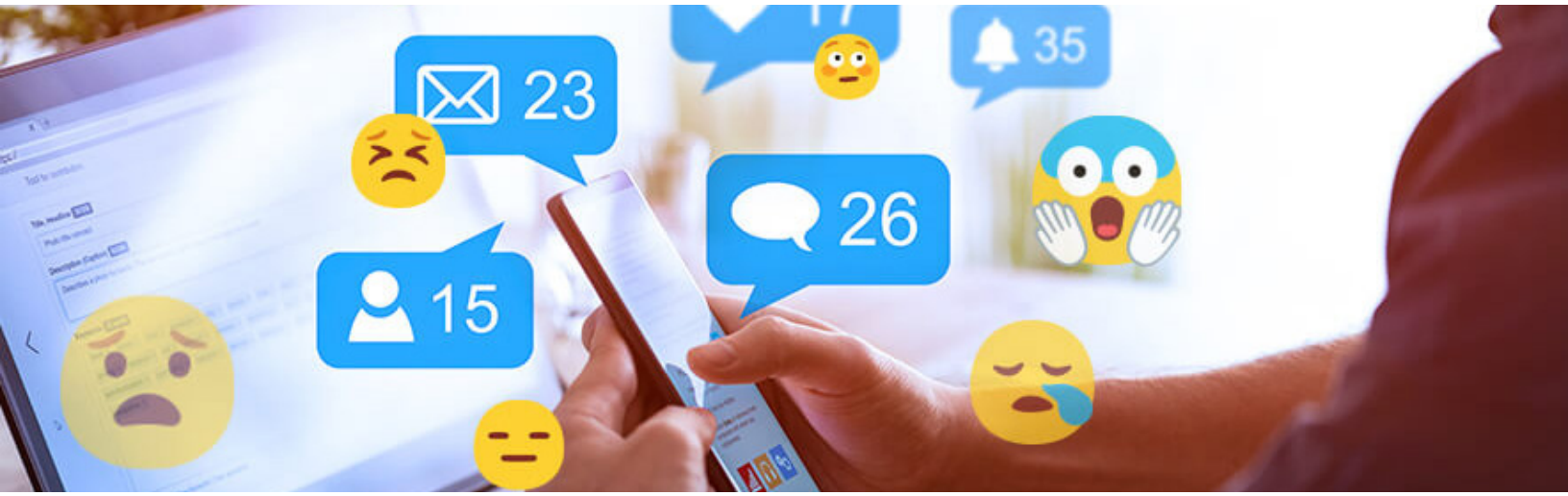
An employer's duty of care must be balanced between an individual's rights and the safety and security of the workplace. Finding that balance in an environment with strong polarized attitudes and opinions is a challenge made more complicated by evolving political and media landscapes. Security professionals must be able to see through the smoke of extreme ideas to determine if the fire of extreme action is being ignited within their workplace.

STEVEN CRIMANDO IS THE PRINCIPAL OF BEHAVIORAL SCIENCE APPLICATIONS LLC, A TRAINING AND CONSULTING FIRM FOCUSED ON HUMAN FACTORS IN CRISIS PREVENTION AND RESPONSE. HE IS A CERTIFIED THREAT MANAGER (CTM) AND A CONSULTANT FOR CORPORATIONS, GOVERNMENT AGENCIES, POLICE, AND MILITARY PROGRAMS.

SECURITY MANAGEMENT

Employee Activism as a Risk Management Opportunity

The combination of increased activism and elevated divisiveness presents a heightened threat for conflict entering the workplace, particularly for corporations whose employees are returning to the office after working remotely.



Preparing for the probability that employees, or those with whom they interact, will offend one another is a logical modern risk management strategy.

Hyper-polarization, fueled by misinformation and the mainstreaming of fringe beliefs, has significantly increased the likelihood that individuals in the workplace will disagree on emotionally charged issues—particularly if the content has been politicized.

Political activism has hit record highs. In the United States alone, Civis Analytics estimates that 23 million residents engaged in some form of protest during 2020, the largest numbers in recorded history. Sources for political information also changed during the past couple of

years. Increasing numbers of individuals now rely on social media platforms for their political news, despite widespread distrust of social media platforms as sources of truth, and heightened awareness of the ways in which social media algorithms amplify polarization, found researchers for a study in *Proceedings of the National Academy of Science*.

As more people become locked inside their own echo chambers, political perspectives often deteriorate into partisanship, and conflict can arise when engaging with those of differing views.

For example, a 2020 Pew Research Survey found that nine in 10 Americans said there is strong conflict between those of different political parties.

The combination of increased activism and elevated divisiveness presents a heightened threat for conflict entering the workplace, particularly for corporations whose employees are returning to the office after working remotely.

These threats can take several forms.

As many corporations have learned, the workplace itself can become the object of employee activism if the workforce believes that the organization can—and should—do more about particular causes.

In the aftermath of a mass shooting at one of its stores, Walmart employees conducted walk-outs to protest the chain's gun sales. Google employees also staged walkouts to protest lack of executive action on claims of gender discrimination and sexual harassment. And when cryptocurrency firm Coinbase attempted to stifle workplace activism by censoring dialogue not related to the corporate mission, 60 employees reportedly quit the company causing the directive to go viral.

Reputational damage and loss of talent are two promi-

nent threats posed by employee activism. But the strategy to mitigate them should not overshadow the opportunity to fortify an organizational culture of safety, engaging in the challenge of accepting diversity of opinion without generating animosity.

Security professionals are positioned to play a key role in proactively assisting executives to manage employee activism in a manner that minimizes conflict and disruption.

An effective strategy relies on human intelligence—listening and gleaning information on the current priorities and perspectives of the workforce. True human intelligence requires emotional intelligence, relationships, and trust, which necessitates a security force that is well-integrated with, rather than siloed from, the workforce.

This information becomes the basis for strategic decision making. Different tactics are suggested by various findings. If there is general cohesion of thought among those within the company environment, there is an opportunity to strengthen workforce loyalty by subtle or overt forms of support for shared causes. These acts—from simple (mentioning the issue in a corporate newsletter) to significant (financial investment in an organization that supports a key issue)—can strengthen staff loyalty, a trait that supports workplace safety. Loyal employees are more likely to report unsafe conditions, comply with safety protocols, and resist unsafe or criminal activities.

If great disparity exists among employees, enlisting experts to help facilitate difficult dialogues models tolerance for non-disruptive engagement. Should the corporation be the target of advocacy—such as when Goya Foods was subject to a boycott for its CEO's political comments or the backlash against Dr. Seuss Enterprises for deciding against reprinting a few of its titles due to racist depictions—identifying the informal advocate leaders in the workforce and

initiating solution-focused conversations between these individuals and corporate leadership—even if what is being sought is not achievable—can assist in building trust, which is foundational for conflict resolution.

Clear communication of behavioral expectations for employees who experience significant disagreement is also an important part of a risk management strategy. Such expectations—which should be congruent with corporate culture—can span a continuum from pausing engagement in non-work-related discussions that cause disruption until a formal forum can be scheduled to the expectation that differences of opinion will be tolerated and respectful listening or disengagement are required.

Explicitly communicating these expectations in a statement that reinforces the corporation's general commitment to diversity and intolerance for discrimination and harassment helps employees navigate a potentially divisive environment before it devolves into a more serious, conflicted one.

Decisions regarding workplace tolerance of visual displays—such as activist email signature blocks, Zoom backgrounds, and office décor—should also be explicit to preempt misunderstandings. Likewise, the workforce should be educated about general policies related to making public statements or participating in acts of civil unrest while wearing corporate insignia.

As with any risk management strategy, the tactics adopted as part of activism risk management need to reflect the culture and goals of the larger organization. And, as many corporations have learned in the past several years, when it comes to activism, the corporate culture may also need to expand to align with a more socially and politically engaged workforce.

AN EXERCISE IN APPLYING CONTEXTUAL INTELLIGENCE

By using the COPE (Culture, Organizational values, Politics, and Environment) framework to assess security challenges and potential flashpoints, leaders can help their institutions navigate complex situations and mitigate reputational risks. For a glimpse of this framework in practice, see the hypothetical case study below.

Entity. A small, rural liberal arts college in the United States with 700 students, 150 core and adjunct faculty, and 80 staff.

Challenge. A university that prides itself on diversity of thought and freedom of expression—and is legally bound to respect civil liberties and academic freedom—is experiencing increased incidences of campus disruption and conflict as students, staff, and faculty vocalize opposing views both on and off campus. The incidents are compromising the quality of campus life. Some in the campus community have reported that they are fearful that the conflict will become violent.

COPE FRAMEWORK ANALYSIS

Culture. Although a comparatively liberal work environment (flexible work schedules, relaxed dress code), the college's employees and students represent diverse populations along every demographic. There is a shared belief in the value of education, although opinions vary as to whether education should principally advance societal or individual goals.

Organizational Values. The college has a strong and well-articulated commitment to diversity and inclusive excellence. Its core mission also includes supporting its graduates to apply the education they gain to resolve complex, real-world situations.

Politics. Prior to the amplified social and political polarization of the past several years, the college frequently confronted divisions among students, faculty, and staff with different worldviews. The use of words such as "safe spaces" and "triggers" are common when individuals are confronted with encounters or material that range from the uncomfortable to the legally unacceptable.

There are several lingering conflicts that have resulted from the perception that the college has "done nothing" in relation to protected actions by some within its constituencies. Additionally, security is aware that students in the emergency management program—which include a significant number of veterans and law enforcement-affiliated students—are feeling that the college is responding unevenly to some of the national events involving BIPOC individuals and the police.

Environment. The college is subject to U.S. state and federal laws related to harassment, discrimination, and Title IX. Faculty are also covered by a collective bargaining agreement and, consistent with academic institutions generally, enjoy broad freedom of expression under the concept of academic freedom.

Determination. The college holds monthly town halls for students, faculty, and staff. It determined that, on a quarterly basis, the college president will make the following points during his remarks:

The college is committed to diversity, explicitly including diversity of thought and expression.

Tolerance does not include tolerating the intolerable. The college will not tolerate harassment or discrimination—as legally defined—and any staff, student, or

faculty member who believes they might be experiencing it such should contact human resources or an office of student affairs.

When disagreements arise, individuals are expected to listen respectfully or disengage.

The college also determined that the diversity officer would create a reporting system for individuals who believed they experienced bias or microaggression, which a cross-disciplinary team would investigate. Additionally, the Title IX officer would partner with security to adapt the school's sexual assault bystander intervention program to train staff on ways to effectively intervene if they witness a disagreement devolve into an argument.

Finally, the college's chief academic officer and a few faculty members met with students from several programs, including emergency management, and scheduled a series of panel discussions involving law enforcement, local government officials, and community advocates to discuss local dynamics related to community policing.

MICHAEL CENTER IS THE UNITED NATIONS SECURITY ADVISER TO BELGIUM, FINLAND, GERMANY, IRELAND, MALTA, MONACO, NORWAY, PORTUGAL, SPAIN, SWEDEN, AND THE UNITED KINGDOM. HIS EXPERIENCE IS FOCUSED ON SECURITY RISK MANAGEMENT IN HIGH-RISK, COMPLEX HUMANITARIAN AND CONFLICT ENVIRONMENTS. AS THE UNDSS HEAD OF OFFICE, CENTER SERVES AS LIAISON BETWEEN THE UNITED NATIONS, HOST GOVERNMENTS, AND THE DIPLOMATIC COMMUNITY TO STRENGTHEN ANALYSIS AND CRISIS MANAGEMENT PREPAREDNESS FOR UNITED NATIONS PROGRAMS. CENTER IS THE CHAIR OF THE ASIS INTERNATIONAL EXTREMISM AND POLITICAL INSTABILITY COMMUNITY.

DIANA M. CONCANNON IS THE DEAN OF THE CALIFORNIA SCHOOL OF FORENSIC STUDIES AT ALLIANT INTERNATIONAL UNIVERSITY, WHERE SHE ALSO SERVES AS ASSOCIATE PROVOST FOR STRATEGIC INITIATIVES AND PARTNERSHIPS. SHE IS A FORENSIC PSYCHOLOGIST AND MAINTAINS A THREAT ASSESSMENT AND MANAGEMENT CONSULTANCY. SHE IS AUTHOR OF *KIDNAPPING: AN INVESTIGATOR'S GUIDE* AND *NEUROCRIMINOLOGY: FORENSIC AND LEGAL APPLICATIONS, PUBLIC POLICY IMPLICATIONS*. CONCANNON IS THE CO-VICE CHAIR OF THE ASIS INTERNATIONAL EXTREMISM AND POLITICAL INSTABILITY COMMUNITY.

THE VIEWS EXPRESSED IN THIS ARTICLE ARE THE AUTHORS' OWN AND ARE NOT REFLECTIVE OF THEIR ORGANIZATIONS.

SECURITY
MANAGEMENT

Reimagining Security in a Post-2020 World

Integration into the workforce environment, rather than mere patrol of it, is more necessary than ever for an accurate assessment, prevention, and disruption of threats.

In 2020, everything changed. More than 100 countries instituted full or partial lockdowns. Workplaces went remote. Schools closed. Disinformation became a thriving industry. Disparities accelerated. Extremism mainstreamed. Geopolitical tensions were amplified by the rising global challenges posed by the pandemic, migration, climate change, and cyber insecurity.

Conflict and violence—ever present in human interactions also changed in 2020. Differences and divides around even the most mundane matters—from mask wearing to mail-in ballots—became sources for passionate debate, and significant issues such as racism, nationalism, and personal liberty spawned spontaneous and

coordinated unrest. The transnational threats of the last 20 years have been supplanted by domestic versions; domestic militants form, disband, rebrand, and reconstitute monthly. Tactics and techniques now include the use of drones, street fighting, and online threat campaigns.

Conversations about the new normal have been had in a myriad of contexts, but there does not seem to be a consensus about what this will entail beyond a continuation of changes in the ways we act and interact.

Maintaining safe environments amid the complex dynamics of our contemporary reality necessitates redefining security and reimagining the role of security professionals. The policing functions of security—gates, kiosks, uniforms, and weapons—leads to stove-piping, creating physical and mental barriers or even polarization between the workforce and security personnel. The traditional focus on access control, protection, psychological deterrence, and emergency response must evolve to align with the more holistic Enterprise Security Risk Management (ESRM) guidelines, such as those published by ASIS. Integration into the workforce environment, rather than mere patrol of it, is more necessary than ever for an accurate assessment, prevention, and disruption of threats.

Working with leadership to evaluate risk tolerance, which may have evolved with the events of 2020 or because of fundamental changes in the work environment, is also important. Remote work habits in particular render it vital to ensure that the workforce is knowledgeable of and invested in the security behaviors that will protect third-party access to organizational systems and assets.

For security initiatives to succeed in today's climate, the broad definition of "stakeholder" envisioned by the ESRM

guidelines must include a wider segment of the workforce, consumer base, and partners. Security professionals are more effective when exposed to the full spectrum of an organization's operations, interests, and security concerns, including active shooter, insider threats, and hate speech in the office.

Cultures of safety must be created to proactively protect assets—people, physical, cyber, and reputational—against both historic threats and those newly introduced by heightened levels of divisiveness and grievance. The security professional-as-partner model is essential to identifying threats and managing risks that can arise from without, as well as those that can materialize within.

The policing functions of security—gates, kiosks, uniforms, and weapons—leads to stove-piping, creating physical and mental barriers or even polarization between the workforce and security personnel.

Reminding staff about incident reporting protocols and adopting modern best practices that focus on intervention rather than surveillance and enforcement, for example, can elevate workforce engagement in security.

Educating the workforce on behavioral indicators associated with contemporary threats—such as colleagues voicing beliefs that violence is the only solution for a particular issue; sudden secretiveness surrounding activities; or new and significant interest in acquiring materials that can be used in an attack—can improve workforce safety literacy and support a more robust partnership.

We must train up and train out.

Given the ubiquitous nature of interpersonal conflict,

security forces—whether contract or proprietary—must be competent in the basics of de-biased decision-making, conflict de-escalation, incident reporting, and recognizing burnout, each of which is vital to accurate assessment and mitigation of disputes. They must be socialized to an organization's values, priorities, and risk management strategy; critical thinking is—more than ever—an essential tactical tool. Providing context helps employees to be mindful of events to report or about which to seek consultation.

Workforce professionals also become part of the solution when they serve as members of mini cross-disciplinary risk management teams. This further elevates their engagement and the proficiency and consistency of staff responses to early alerting to, potentially preventing, and more effectively mitigating threats and risks. Highly visible threat management teams in which staff join traditional members—human resources, security, legal, communication, and threat assessment professionals—also encourage valuable intelligence reporting by non-team members, supporting risk mitigation efficacy.

This effort is a force multiplier that enhances security effectiveness. Rapid societal change creates new threats that exploit previously unrealized vulnerabilities. Broadening the conversation and expanding participation help to identify security risk gaps and blind spots.

The events beginning in 2020 surfaced a truism of human behavior: For an organization to be secure, all members of the community need to feel safe. And to build that culture of safety, security professionals must move beyond the role of responders and enforcers and into the role of educators, partners, and leaders.

DIANA M. CONCANNON IS THE DEAN OF THE CALIFORNIA SCHOOL OF FORENSIC STUDIES AT ALLIANT INTER-

NATIONAL UNIVERSITY, WHERE SHE ALSO SERVES AS ASSOCIATE PROVOST FOR STRATEGIC INITIATIVES AND PARTNERSHIPS. SHE IS A FORENSIC PSYCHOLOGIST AND MAINTAINS A THREAT ASSESSMENT AND MANAGEMENT CONSULTANCY. SHE IS AUTHOR OF *KIDNAPPING: AN INVESTIGATOR'S GUIDE* AND *NEUROCRIMINOLOGY: FORENSIC AND LEGAL APPLICATIONS*, PUBLIC POLICY IMPLICATIONS. CONCANNON IS THE CO-VICE CHAIR OF THE ASIS INTERNATIONAL EXTREMISM AND POLITICAL INSTABILITY COMMUNITY.

ANTHONY MCGINTY, CPP, IS A CONSULTANT AND INTELLIGENCE ADVISOR BASED IN GREATER LOS ANGELES. HIS FOCUS IS SUPPORTING AND MAXIMIZING SECURITY PROGRAMS THROUGH A STRUCTURED THREAT ANALYSIS APPROACH. MCGINTY'S WORK HAS BEEN FEATURED IN *THE ATLANTIC* AND CNBC. HE IS THE RECIPIENT OF A 2017 LOS ANGELES MAYOR'S CIVIC INNOVATION AWARD.

SECURITY
MANAGEMENT

ASIS INTERNATIONAL
Advancing Security Worldwide®

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

To join ASIS International and become a subscriber to *Security Management*, visit asisonline.org/membership/join.