everbridge®

WHITE PAPER

# When Risk Comes Home: Out of Sight Cannot Mean Out of Mind

## A 10-POINT PLAN FOR PROTECTING EMPLOYEES WORKING FROM HOME

The U.S. has become a work-from-home (WFH) economy, now accounting for 60% of U.S. economic activity

In 2016, the research firm IDC predicted that the number of remote workers in the U.S. would rise from 96.2 million to 105.4 million over the following five-year period. They estimated that by 2020 mobile workers would account for nearly three-quarters (72.3 percent) of the U.S. workforce. Even the best and brightest analysts could not have accurately forecast a devastating pandemic that would shut down economies around the globe. Government "stay-at-home" orders in response to the COVID-19 public health crisis has resulted in completely reshaping the contemporary work environment.

The new working-from-home environment is predicted to continue long past the coronavirus pandemic that spawned it, and the crisis poses new challenges – from a ticking time bomb of inequality to an erosion of city centers – according to Stanford economist Nicholas Bloom. The U.S. has become a work-from-home (WFH) economy, now accounting for 60% of U.S. economic activity. Almost twice as many employees are working from home as at traditional workplaces.

This reality is also reflected internationally. A Gartner, Inc. survey of 800 global HR executives in March found that 88% of organizations had encouraged or required employees to work from home, regardless of whether or not they showed coronavirus-related symptoms. Nearly all organizations (97%) had canceled work-related travel. A survey of 250 large firms in Argentina found, for example, showed that 93% had adopted teleworking as a policy in response to COVID-19.

In another survey conducted by 451 Research and S&P Global Market Intelligence, close to 80% of organizations reported that they had implemented or expanded universal work-from-home policies as a result of COVID-19, and 67% expected those policies to remain in place either permanently or for the long-term. At this point, there may be no turning back. Even when the pandemic threat dissipates, employees are likely to demand a work-from-home option, or at least the availability of a hybrid approach, blending working from the home and office. There are pros and cons for both employers and employees in work from home arrangements. Those most commonly reported include:

### PROS

+ Better work-life balance
+ Less time on the road (safer, less stressful)
+ Greater productivity
+ Positive environmental impact
+ Money saved (by all parties)
+ More job satisfaction
+ Less sickness
+ More time for fitness
+ Improved inclusivity-diversity of workforce

### CONS

+ Increased isolation
+ Home office costs
+ Risk of overworking
+ Risk to productivity
+ Distractions at home
+ Workplace disconnect
+ Less face time

While less obvious, there is another important feature of this shift in where work is done; that is the corresponding shift in work-related risks that can follow employees to their homes.

## IT IS THE EMPLOYEE'S HOME, BUT THE EMPLOYER'S WORKPLACE

As the nature of workplace has changed, so has the nature of work-related risks. Those risks, both physical and psychological, like the workplace itself, are quickly evolving. The organization that has required employees to work from home has by extension created at workplace at their employees' residence. The employer who has purchased ergonomic chairs or desks, and pays for Internet service has helped establish the employee's home office as a workplace, and while it may be the employee's home, it is the employer's workplace. As such, workplace risks shift from the corporate office to the private residence.

While attempting to mitigate the risk of COVID-19, employers must ensure that working conditions do not deteriorate.

Home-based workers have the same workers' compensation benefits as those working on the employer's premises. Cases regarding workers' compensation have shown that the law tends to see the home office no differently from the office building. While OSHA does not have a specific regulation regarding home offices per se, it is clear that "employers have a 'general duty' to provide their employees with a workplace free from recognized hazards likely to cause death or serious physical harm." For OSHA the term "workplace" is synonymous with "on the job" and "at work." A workplace may be any location, either permanent or temporary, where an employee performs any work-related duty.

While attempting to mitigate the risk of COVID-19, employers must ensure that working conditions do not deteriorate. The International Labor Organization's (ILO's) Home Work Convention, 1996 (No. 177) calls for equality of treatment between homeworkers and other wage-earners in relation to wages and benefits, access to training, occupational safety and health (OSH), and social protections. The convention applies to employees who perform their work at home on a regular basis, and with so many employees working from home daily, WFH in the current environment would likely be considered within the scope of C177.

All employers owe a Duty of Care to their employees, regardless of where they work. That Duty of Care extends to physical and mental injuries, including work-related stress. Those working at home should not be at more risk than other employees in the organization. Fulfilling a Duty of Care means that the employer should take all steps which are reasonably possible to ensure the health, safety, and wellbeing of their employees. If an organization does not meet this standard of care, then its actions or inactions could be considered negligent, and any damages resulting may be claimed for negligence.

There are a range of potential risks associated with the work from home environment that require forethought and attention. These include:

1. Cyber Security: Virus and malware, phishing emails, WiFi vulnerability, etc.
2. Information Security: Physical files and data (hard copy, on storage devices, etc.)
3. Electrical Safety: Home system is adequate for demand, surge protectors, cord management, outlets, switches, etc.
4. Fire Safety: More than one way out of work area, clear ingress/egress, smoke/carbon monoxide, fire extinguisher, space heaters, free of clutter-combustible materials, etc.
5. Structural Safety: Adequate ventilation/heating/cooling, file cabinets are not top heavy, cabinets, shelves or furniture greater than 5' high are secured to prevent toppling, etc.
6. Ergonomic Safety & Health: Lighting, seating, desk, monitor, keyboard, etc.
7. Psychological Safety & Health: Distractions, loneliness, isolation, stress, anxiety, person/role conflict, etc.
8. Physical Security: Robbery, theft, domestic violence, work-related violence (bullying, harassment, threats, physical violence, etc.)

Workplace violence is a perennial threat, and even in the COVID-19 environment that has not changed. What has changed is how and where violence can occur.

## VIOLENCE AS A FORESEEABLE RISK

Safety and security do not begin and end at the walls of an employer's facilities or the perimeter of their parking lots. The employee working from home may still incur a number of risks, including a risk of violence, as well as other hazards, but typically does not enjoy the same physical security apparatus or violence prevention programs and practices as in the traditional workplace, thereby creating a perfect storm of risk. These risks may threaten not only the employee, but their families and others in their homes. The principles of workplace safety, security, and violence prevention must be adapted to the home office environment to help reduce the likelihood and severity of potential emergencies. Workplace violence is a perennial threat, and even in the COVID-19 environment that has not changed. What has changed is how and where violence can occur. Given the grim statistics of those killed and injured on the job each year, violence is certainly a foreseeable risk in all types of work. No occupation or work site is immune from this risk, even when employees are working from their own homes.

Incidents of workplace violence are already thought to be greatly underreported. Violence occurring in the home office setting may not be immediately recognized or reported as workplace violence. Police reports, news stories and employer safety logs may describe such incidents as home invasions or burglaries, incidents of domestic violence, or sexual assaults. But if such violence occurs while the worker is on the clock, they may also be instances of workplace violence. As such, safety, security and violence prevention measures applied to the home office environment can help reduce the likelihood and severity of such incidents, and can help manage this risk for both employers and employees.

## IT'S ABOUT THE RELATIONSHIP, NOT THE ENVIRONMENT

One of the greatest lessons in the annals of crisis management was articulated by the 9/11 Commission in the wake of the catastrophic terrorist attacks in 2001. A central finding of the Commission was that, "The most important failure [concerning the 9/11 attacks] was one of imagination." The members of the group determined that national security leaders and emergency managers failed to envision and anticipate the event that would so change our world. Leaders in the current global crisis cannot repeat this mistake. When envisioning potential workplace violence scenarios that can affect employees working from home, employers must consider all sources and types of violence, including the four traditionally recognized by OSHA, and a fifth type that has become a reality in the post-9/11 world. By becoming familiar with the various types of workplace violence, employers can better imagine how these might apply to the home office environment.

The various types of workplace violence are not defined by the manner of violence, or even where it occurs, but rather by the real or perceived relationship between offenders and their victims. In a WFH arrangement, the relationships employees and customers, employees and other employees or supervisors, employees and domestic partners, and others do not necessarily end when employees stop working at the company office and begin working from the kitchen table. All five types of workplace violence may still pose a risk to the WFH employee.

### Type I: Criminal Intent/No Legitimate Business Relationship

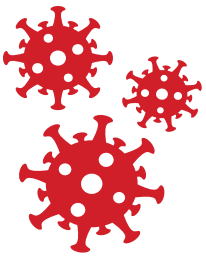
Type I violence is perpetrated by a stranger usually in the context of a robbery, theft or trespassing. Those workers who routinely transport pharmaceutical or jewelry samples t have always been potential targets of Type I violence at their homes. An employee may set up their home office in front large picture window to enjoy the view and sunlight while working. From outside, others can easily see the worker's desk, computers, and other electronic devices, as well as learn their work routine, making the home office an attractive target for a would-be robber.

### Type II: Patient, Client or Customer

While it might be an organization's policy and practice that home workers should never allow clients to visit their home-based office, a determined client, especially one energized by anger or frustration, can easily find where an employee is working. GPS tracking, Internet searches of public records and documents, and geotags in photographs posted online, all can create a trail leading right to the worker's doorsteps.

### Type III: Co-worker to Co-worker

Through the same tracking means mentioned above, or by way of their work relationships, current and former employees may know or can find where an another employee lives. Visiting a current or former employee or supervisor at their home office with anger or aggression in mind is a foreseeable situation. There have been several instances in which angry employees simply followed co-workers or supervisors home, and in both overt and covert ways, terrorize the targeted employee and their family members.



Victims may also not have the same options to seek refuge with friends, family or shelters for fear of spreading or being exposed to the COVID-19 virus.

### Type IV: Intimate Partner/Domestic Violence

Domestic or intimate partner violence following an employee from home to the workplace is a recognized and tragically common form of workplace violence. Such violence can and does visit the workplace, often with devastating consequences. This has historically been a tricky issue for employers, but it is clear that an employer who knew or should have known that their employee was at risk does have an obligation to intervene.

While employers are increasingly recognizing and addressing the possibility of an estranged spouse or partner targeting an employee at the organization's offices, fewer have considered the risk of this type of violence affecting someone working from a home office. Intimate partner or domestic violence victims may no longer have the safe haven of leaving the home each day for work, and for many, levels of financial and interpersonal stress have increased as people have been forced to work from home for weeks or months at time. Victims may also not have the same options to seek refuge with friends, family or shelters for fear of spreading or being exposed to the COVID-19 virus.

Intimate partner violence is all about power and control, and when isolated to their homes with greater exposure to their abusers, victims can be at greater risk with fewer resources. In some instances, working from home may increase the risk and reduce the employer's ability to be helpful by developing a safety plan or hardening security at their facilities.

### Type V: Ideological Violence

OSHA has long-held that there are only four types of workplace violence. In the post-9/11environment, most workplace violence prevention authorities recognize that ideological violence directed at an organization's people or properties, because of what the organization does or what it represents, is a real and significant risk worthy of being recognized as its own type. Type V violence occurs at the intersection of workplace violence and terrorism. The previous and most recent attacks directed at Charlie Hebdo's offices and employees in Paris, the Planned Parenthood clinic in Colorado Springs, and the San Bernardino Public Health Department, were all ideologically-motivated-they were also all work related.

This risk began well before the 9/11-era. A well-known example would be that of Thomas Mosser, an advertising executive killed in his home by the Unabomber because of his firm's work on rehabilitating Exxon Mobile's reputation in the wake of the Valdez oil spill. Mr. Mosser was simultaneously a victim of domestic terrorism and workplace violence. He was targeted because of the nature of his and his employer's work, and what his firm represented. Mr. Mosser was not a random victim; this was an instance of targeted violence. One of the most frightening aspects of this case was that the violence found its way to Mr. Mosser's home, with his wife, one of his children and her friend in adjacent rooms at the time of the blast. Without dwelling on the details of the bomb or its impact, it is sufficient to say an attack against an employee in their own home is beyond traumatic. At the time, it seemed unimaginable, and that attack occurred in the pre-Internet world where it was not nearly as easy to find where someone lives.

Employers concerned with safety, security, and the defensibility of their actions must consider opening the umbrella of their workplace violence prevention policies and programs wide enough to cover employees working from home offices.

The Unbomber attack on Tom Mosser was in 1994. In July 2020, an attorney known as a militant anti-feminist, showed up at doorstep of U.S. District Judge Ester Salas in North Brunswick, New Jersey home. Dressed in a FedEx uniform, Roy Den Hollander opened fire, killing the judge's 20-year old son and seriously injuring her husband. Hollander once argued a case before Salas, and was a vocal men's rights activist with a history of threatening the use of violence against powerful women. Tragically, this is another clear example of Type V violence motivated by an extreme ideology, and of how violence related to one's work can and does find its way to the home.

Consider the employee who works for a life science or biotech company engaged in controversial work who may be targeted by environmental or animal rights activists. Extremists within such groups operate with the belief that the small harm that they inflict may be necessary to prevent a perceived larger harm from being done by the company. Targeting the offending organization or its employees wherever they may be is often within the scope of acceptable options for the extremist group or true believer who feels that violence is both justified and necessary.

Our world has not become more peaceful or less vulnerable to terrorism since the days of the Unabomber. Type V violence can be directed at employees in their home offices, as well as in the traditional workplace. Reviewing the five types of workplace violence that should concern employers, it is important to understand that no organization is immune from any or all of these risks. Certain industries and jobs may present higher risks for certain types of violence, but it cannot be assumed that these threats do not apply to all organizations in some way.

It is also important to note that all five types of workplace violence are based upon the relationship between the targeted employee(s), organization(s), and the attacker(s). The types of violence have no relationship to where the incidents occur, rather it is about who perpetrates the violence and their relationship to their victim(s). Working from a home office does not change the relationship, real or perceived, between the violent actor and the targeted employee. Working, perhaps alone at home, may just make someone more vulnerable. At the home office, there is not a mail room screening for suspicious packages or security guards checking IDs of those arriving at the doorstep. When transitioning from the organization's offices to the employee's home office, the security risks remain, but the security resources are often left behind.

Employers concerned with safety, security, and the defensibility of their actions must consider opening the umbrella of their workplace violence prevention policies and programs wide enough to cover employees working from home offices. In the words of the renowned law enforcement instructor, Gordon Graham, "If it is predictable, it is preventable." Violence has become a foreseeable risk in the modern workplace, but the place where modern work is done has changed. It has been changing slowly for some time, but that change accelerated dramatically in response to the COVID-19 pandemic. Some of that change may be here to stay, so it will be important for all those tasked with workplace violence prevention to anticipate the possibility of violence occurring in an employee's home office and help employees implement effective countermeasures to mitigate that risk.


The 10-point plan described in the following pages can provide a road map for employers and employees in ensuring a safe, secure, and violence-free workplace for those working from home.

## MITIGATING THE RISK OF VIOLENCE FOR THE WFH WORKFORCE

Among the numerous risks that can affect employees working from home, the risk of violence to employees, wherever they may be working, is well-recognized. Approaches to mitigating this risk have been offered by OSHA for many years as "guidance's," but the creation of a national standard specific to workplace violence created a clear pathway for employers to develop and implement workplace violence prevention programs. The American National Standard for Workplace Violence Prevention and Intervention articulates the elements of an effective and defensible approach to violence prevention for employers of all types. The standard, a creation of the Society for Human Resource Management (SHRM) in partnership with the professional security accreditation organization, ASIS International, has quickly become a touchstone in the plaintiff's strategy for workplace violence-related litigation, and should guide the workplace violence prevent efforts for all kinds of workers in all types of settings.

Employees working from home may experience a number of other factors that can increase their risk. Among them are complacency and decreased situational awareness, as well as the illusion of safety in their homes. There are multiple cognitive biases that can influence risk perception and reduce an employee's level of vigilance when working in the comfort of their own home. In most instances a residential setting is typically a "soft target" with minimal physical security. The presence of dependents (children, elderly care, etc.) in the home changes the risk equation, and since others in a home may not be able to assist in an emergency, they may in fact, make the employee less likely to effectively respond to a hostile encounter or dangerous situation. There are also may distraction in and around the home. Employees may have to balance working with family or pets who are also in the home, performing routine household chores during the workday, or even getting distracted by television and other personal electronics at their disposal. Such distractions can lead to missing the indicators of risk.

The challenge then, is adapting the principles established in the various OSHA guidelines and the national standard to this challenging workplace, where it would seem that an employer would have much less control. The 10-point plan described in the following pages can provide a road map for employers and employees in ensuring a safe, secure, and violence-free workplace for those working from home. Safety and security are always a shared obligation, both the employer and employee must do their parts. By working together, the risk of violence can be effectively managed.

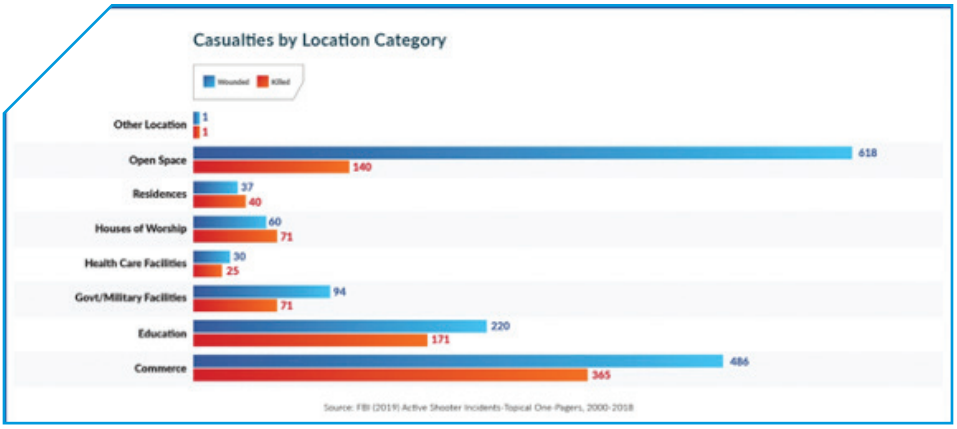
## THE 10-POINT PLAN

### Step 1: Secure Executive Support

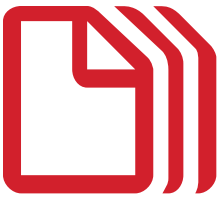
Leaders must first and foremost understand and accept that workplace violence is a serious problem that can have a devastating impact on employees and the organization. Workplace violence threatens employee safety, morale, and retention, as well as an organization's brand and reputation. In 2014, Liberty Mutual reported that workplace violence cost U.S. employers an estimated $121 billion per year. More than 876,000 work days were lost, costing employees more than $16 million in lost wages. When violence on the job resulted in litigation, the average out-of-court settlement was $500,00.00, with jury awards ranging up to $3 million. Few crises are as damaging and costly for employers, never mind the human cost in pain and suffering.

Leaders must envision the possibility of violence affecting the home office worker, and afford home-based employees the same protections as those working in traditional office environments. Employers of people who work from home offices and may be isolated during their work time must take reasonable steps to minimize the associated physical and psychological risks. Organizations that promote home office safety typically address a range of issues such as ergonomic risks and electrical safety, but seldom mention the risk of violence, other than recommending that visits with clients should take place in public places like coffee shops, rather than at the worker's home office. There is a much wider array of risks than tripping over loose wires or neck and back strain. Physical and psychological risks, including the consequences of isolation and increased relationship stress in the home, can also threaten employee wellness and productivity.

It is important for leaders to recognize that workplace violence is not limited to gun violence or active shooter incidents. Workplace violence occurs on a continuum ranging from bullying, harassment, and angry outbursts to physical assault, weapons-involved violence, and active shooter incidents. All of these manifestations of violence can occur in the home office setting, as well as traditional workplaces. While gun violence occurring at employee's home is likely to be highly-targeted rather than the type of random target selection often involved in mass shootings, active shooter incidents can and do occur in private homes. An FBI review of active shooter incidents in the U.S. from 2000-2018 document 37 deaths and 40 injuries in private residences.




As with all risk management and violence prevention initiatives, it is critical to first garner executive buy-in. This may be easier for organizations that already have robust workplace violence prevention programs in place since most of the heavy lifting in program development has already been done. Discussions about Duty of Care, OSHA's viewpoint, workers' compensation issues, and the risk factors that contribute to violence potential in home office work, can help inspire leaders to take this problem seriously. As previously mentioned, employers have a Duty of Care for their employees regardless of where they work. Executive managers must get their heads around this concept and understand how it applies to their home office workforce.



When reviewing existing policies, or developing new policies from scratch, consider how workers in non-traditional settings are covered.

### Step 2: Formalize and Integrate Policies & Plans

Having a defined work-from-home policy is a must for any organization that permits employees to work from home. This can help reduce the inherent risks by establishing a set of procedures that employees must follow in order to work from home. A work-from-home policy should include additional information about security practices and outline all employees' responsibilities when it comes to safety and security. Some examples of procedures that should be included in a working-from-home policy include:

+ A process for approving employees to work from home.
+ Defined responsibilities for employees.
+ Guidance on what employees must do to secure their at-home workspaces.
+ Clear workstation and/or device hardening steps (this can be a separate policy or referenced another policy).
+ Outline the procedure for reporting a concern or an incident, should one occur.
+ Approves reimbursing employees for costs incurred for performing work at home, such as home office supplies.

Work-from-home safety, security and violence prevention-related policies should align with relevant security, HR and other policies guiding on-site risks (e.g., harassment, discrimination, cybersecurity, etc.). Employee handbooks and orientation materials should be updated accordingly. If an organization has already developed a sound and defensible workplace violence prevention policy, it is likely that working from home is implicitly covered. Most workplace violence prevention policies include broad language that discusses violence potentially occurring anywhere and anytime an employee is on the clock conducting company business. When reviewing existing policies, or developing new policies from scratch, consider how workers in non-traditional settings are covered. This includes workers in home offices, lone or remote workers, business travelers, travelers abroad and ex-pats. It will also be important to discuss how such policies relate to part-time, per diem, and contract employees-- essentially everyone doing business on the company's behalf.

In addition to ensuring that workplace violence prevention policies envision the risk of violence to home office workers, it is helpful to cross-reference workplace violence prevention policies with work-from-home policies. Integration of violence prevention into home-working policies ensures that this risk will be discussed proactively with any new home office worker, and not simply be assumed to be addressed in general workplace violence awareness training. The development and implementation of procedures for violence prevention, response and recovery will be a necessary step in making policies actionable.

Keep in mind: the pandemic will pass, but policies developed in response to today's challenges may endure. Think beyond the current crisis to lasting work-form-home policies and plans that might be useful in permanent home-office arrangements or in future crises that displace workers or require them to work from alternate sites.

Managers can help address violence risks by establishing structured daily check-ins and rules of engagement, and when to use other methods in urgent situations.

### Step 3: Provide Manager Training

Managers should be knowledgeable about the organization's workplace violence prevention policies, programs and procedures. They should also be aware how these policies relate to work-from-home risks and procedures for ongoing violence prevention and emergency responses to concerns or incidents. Managers can help address violence risks by establishing structured daily check-ins and rules of engagement, and when to use other methods in urgent situations. It is helpful to provide several different communication technology options: Video/audio is helpful to gauge changes in an employee's functioning that may be masked in email and text communications. A manager may notice a change in appearance, demeanor or performance that indicates some type of deterioration in the employee's wellness or home situation that may require intervention. Frequent contacts also provide opportunities for remote social interaction (i.e., informal conversations about non-work topics) which can reduce feelings of isolation, or allow a manager to offer encouragement and emotional support. It is important for managers to acknowledge stress, listen to employees' anxieties and concerns, and empathize with their struggles. It is also important to know when to refer an employee to the EAP or other sources of help.

### Step 4: Provide All-Employee Training

Workplace violence prevention programs rely on a saturation model: every employee needs to be aware of how to identify and respond to a violent situation. Employers count on employees to recognize when a co-worker or client may be on a pathway to violence, and an employee who isn't familiar with the proper response to a "shots fired" alert in the workplace might put themselves and others at risk. Organizations must also provide training for all employees to effectively comply with workplace violence policies governing their conduct while working from home. This includes both introduction to the organization's overall violence prevention policies, programs, plans and procedures, as well as work-from-home-specific risks, polices, plans and procedures. It is also important to discuss how a person or incident of concern may be encountered in the work-from-home environment, since it likely be different from the traditional work setting.

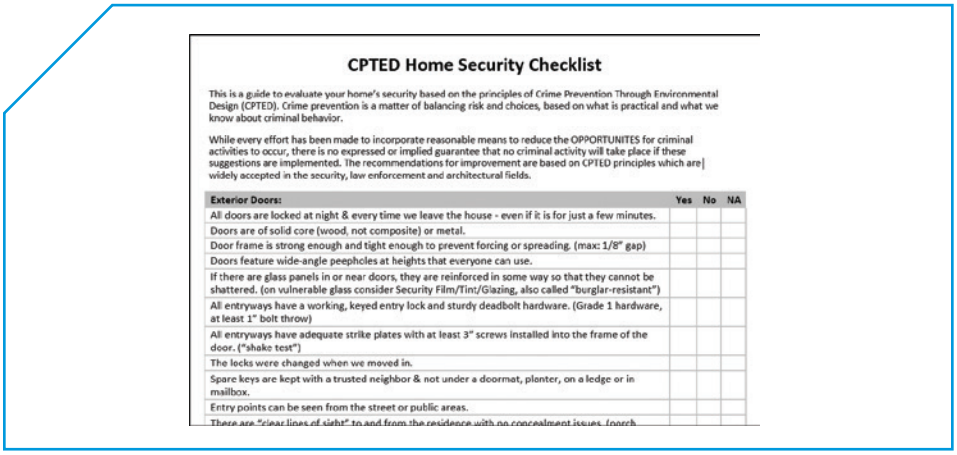
As part of an all-employee training model, it is helpful to provide guidance and resources for securing home and family, including discussions about recognizing risks, such as suspicious people, mail, or vehicles near their homes, as well as developing and rehearsing practical Emergency Action Plans. Employees must also be familiar and practiced in using emergency notifications tools and reaching security support if there is a problem.

### Step 5: Home Safety Self-Assessment

To better understand potential safety and security vulnerabilities, it is helpful for employees to conduct a basic home safety assessment. Organizations can provide tools and guidance for self-assessment of the home, workspace, and employee's level of preparedness to prevent or respond to threats to their safety. Such assessments be focused on general safety concerns, such as fire or storm readiness, or be focused exclusively on home and personal security.

It is important for employees and others in the home to have a safety plan, and be able to quickly execute that plan should there be an adverse event in the work-from-home environment.

Crime Prevention Through Environmental Design (CPTED) is a security concept intended to alter and expand the participants' perception of immediate physical environment. By altering the perception of the physical environment, the participant in a CPTED assessment will be more capable of understanding the direct relationship of the environment to human behavior and crime or violence, as well as other risks. Conducting a self-assessment is also an approach to actively engaging employees in their own safety, after all, safety and security measures work best when they are done with, rather than done for employees. Ultimately, the employee will likely know their home safety vulnerabilities better than anyone else. As a way of documenting this process, employer may require employees to submit a signed attestation that the self-assessment was completed and that they have taken actions to ensure a safe workplace.



**CPTED Home Security Checklist**

This is a guide to evaluate your home's security based on the principles of Crime Prevention Through Environmental Design (CPTED). Crime prevention is a matter of balancing risk and choices, based on what is practical and what we know about criminal behavior.

While every effort has been made to incorporate reasonable means to reduce the OPPORTUNITES for criminal activities to occur, there is no expressed or implied guarantee that no criminal activity will take place if these suggestions are implemented. The recommendations for improvement are based on CPTED principles which are widely accepted in the security, law enforcement and architectural fields.

| Exterior Doors: | Yes | No | NA |
|---|---|---|---|
| All doors are locked at night & every time we leave the house - even if it is for just a few minutes. | | | |
| Doors are of solid core (wood, not composite) or metal. | | | |
| Door frame is strong enough and tight enough to prevent forcing or spreading. (max: 1/8" gap) | | | |
| Doors feature wide-angle peepholes at heights that everyone can use. | | | |
| If there are glass panels in or near doors, they are reinforced in some way so that they cannot be shattered. (on vulnerable glass consider Security Film/Tint/Glazing, also called "burglar-resistant") | | | |
| All entryways have a working, keyed entry lock and sturdy deadbolt hardware. (Grade 1 hardware, at least 1" bolt throw) | | | |
| All entryways have adequate strike plates with at least 3" screws installed into the frame of the door. ("shake test") | | | |
| The locks were changed when we moved in. | | | |
| Spare keys are kept with a trusted neighbor & not under a doormat, planter, on a ledge or in mailbox. | | | |
| Entry points can be seen from the street or public areas. | | | |
| There are "clear lines of sight" to and from the residence with no concealment issues. (porch | | | |

Sample CPTED Home Security Checklist

## Step 6: Develop & Rehearse Emergency Action Plans

Anyone likely to be in the home, once a home also becomes an office, must be involved in a discussion about safety and violence prevention. This includes children, elders, and anyone who can be affected by an unwelcomed visitor or hostile encounter in the home office setting. Family members and others in the home can be a distraction at times, but they can also be potential targets or assets in terms of safety and security during a difficult or dangerous situation.

It is important for employees and others in the home to have a safety plan, and be able to quickly execute that plan should there be an adverse event in the work-from-home environment. Everyone who is routinely in the home should be familiar and capable of initiating the plan. Such plans should include agreeing to who goes to or opens the door when an unfamiliar visitor arrives; how an angry encounter at the home will be handled; and knowing and practicing an escape/evacuation plan, as well as a shelter (i.e., a safe room with solid locking door, sufficient cell phone signal, etc.) response to a hostile encounter. It is helpful to also have agreed-upon code words if it becomes necessary to communicate covertly during a threatening situation. Such conversations should be conducted in age-appropriate ways, not to scare others, but to help them become active participants in home office safety.

For any type of emergency, including violent situations, employees must have access to rapid, reliable tools to send and receive alerts, as well as threat-related information.

### Step 7: Promote Threat Recognition, Reporting, Assessment, & Management

Employees must be knowledgeable about their employer's approach to threat assessment and management. If the organization has a well-developed Threat Assessment and Management (TAM) team or process, it is important for everyone to understand when and how to use it. Employers must therefore be prepared to received and act upon information pertaining to a concern at an employee's home office. If not already implemented, consider forming a multidisciplinary team to respond to reports. Team members may include representatives from human resources, risk management, security, and legal, as well as third-party consultants and subject matter experts.

Employees should be familiar with the pre-incident indicators of aggression or violence, and understand how those indicators might be somewhat different during virtual encounters. It is also helpful to understand the signs of hostile surveillance and basic countermeasures. For example, while an executive might hold a virtual town hall meeting from their home as a way of connecting with and supporting the workforce during a time of social distancing, they might not realize that the family photo on the bookshelf behind them in their video conference might provide personal information to a disgruntled worker with hostile intent. Likewise, that video shot from their lap might be showing the layout of their home, the position of doors and windows, or books about their hobbies that might be useful to a skilled social engineer who can exploit such information for criminal purposes. While traditional approaches to detecting hostile surveillance might involve "watching for watchers" on foot or in nearby parked cars, hostile surveillance is different in virtual meetings.

Cyber-bullying and harassment in the online environment are recognized elements of the workplace violence continuum, and should be reported. Employees must know how to report perceived risks and hostile encounters that happen in real life or the virtual work environment.

### Step 8: Develop Crisis Notification & Security Support Mechanisms

For any type of emergency, including violent situations, employees must have access to rapid, reliable tools to send and receive alerts, as well as threat-related information. Employees should know their employer's process or system for emergency notification of an incident in progress or if they need help regardless of where they are. This can be achieved through enterprise-wide applications, code words and phrases communicated by phone or text to the main office (e.g. "Please send the red folder.") or other means. During a crisis, there should be no time lost in sharing critical information. The plan may simply be to call 911, but everyone needs to be aware of how and when to call for help, and what will happen next.

### Step 9: Clarify Incident Reporting

Both employers and employees must be clear on what type of situations should or must be reported, as well as the method(s) to be used to report concerns, threats or incidents. Employees should also know what to expect in terms of confirmation of receipt and/or response time to their reports. Reports can't seem to go into a black box, and employees can't be left feeling like sitting ducks during a threatening situation.

### Step 10: Ensure EAP& Other Supports

Employers must be cognizant of, and prepared to address, the multiple stressors impacting the workforce in the short period of time that has been the COVID-19 pandemic. These stressors may be weighing on an employee's coping mechanisms and increasing both physical and psychological risks. The unprecedented situation may compound and magnify emotional reactions with fear and frustration, and in some instances can result in aggression or violence.

A recent study by the Kaiser Family Foundation showed that a growing number of U.S. adults are struggling with mental health issues related to the coronavirus, increasing from 32 percent in March to 53 percent in July. Those experiencing symptoms of anxiety or depression, for example, reached 40 percent this summer, up from 11 percent a year ago. In addition, a similar assessment from the Centers for Disease Control and Prevention found that 13 percent of adults had started or increased alcohol consumption or drug use to help cope with pandemic-related woes, and 11 percent had seriously considered suicide in the past month.

With large segments of the workforce now working from home, household dynamics can change, sometimes for better, other times for worse. Close quarters with roommates, spouses and partners, or children (all of whom may be working or schooling from home) can create tension. There have been many reports of increased feelings of isolation, fears of illness/death from pandemic, grief and trauma resulting from illness or deaths in a family due to COVID-19, and rampant uncertainty and anger. Increased financial stressors, and struggles with pre-existing mental health and/or substance abuse problems can all be made worse by the pandemic. In addition, the stress from feeling threatened and unprotected from risks at one's own home can be overwhelming.

Dealing with violence-related risks proactively by addressing work-from-home vulnerabilities is important to protect both the physical and emotional health of employees.

The experience of a job-related hostile encounter or violence incident at one's home can be terrifying and traumatic, not just for the employee, but for children or elderly family members in the home. Dealing with violence-related risks proactively by addressing work-from-home vulnerabilities is important to protect both the physical and emotional health of employees.

Employers must ensure that employees have timely access to quality Employee Assistance Program services, or other means of addressing the emotional impact of a near-miss or actual violent situation, as well as the multitude of other pandemic-related challenges. It is important to clarify with contracted EAP providers if they provide in-home services (or just telephonic/video support), if they will provide support to everyone in the home, and how employees can access or request services, as well as the expected time from request to service delivery.

## PULLING IT ALL TOGETHER

Leaders in all types of organization must realize that in the current climate, no one is immune from either the pandemic risk of COVID-19 or the endemic risk of workplace violence. The combined effect of these two threats has created a perfect storm of risk, and both risks can find employees wherever they work. Executives must envision the possibility of violence affecting the home office worker, and afford home-based employees the same protections as those working in traditional office environments. The 10-steps addressed here can serve as framework to help organizations approach the complex challenge of workplace violence prevention during this time of unparalleled complexity created by a devastating global health emergency.

## About the Author

Steve Crimando is the principal and founder of Behavioral Science Applications LLC, an operational risk management consultancy located in the New York metropolitan area. He is a consultant and educator focused on the human element in security, violence prevention, and emergency management.

Steve is a Certified Threat Manager (CTM), Certified Homeland Protection Professional (CHPP) and a Board Certified Expert in Traumatic Stress (BCETS). With more than 30 years of experience in the field, He was deployed to the 9/11 and 1993 World Trade Center attacks, as well as New Jersey's anthrax screening center, and other acts of international terrorism. He is a published author who is frequently called upon by the media and the courts as an expert in violence prevention and response. He provides training and support to programs within the U.S. Department of Homeland Security, U.S. Department of Justice, law enforcement, intelligence and military agencies, as well as NGO's, such as the United Nations.

References:

i. Business Wire (2015). IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020. Retrieved from http://www.businesswire.com/news/home/20150623005073/en#.VYmhfEZB58m

ii. Bloom, N. (2020). How working from home works out. Stanford Institute for Economic Policy Research, Stanford University, Stanford, CA.

iii. Ibid.

iv. March 2020: Gartner HR Survey Reveals 88% of Organizations Have Encouraged or Required Employees to Work From Home Due to Coronavirus. Gartner, Inc. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88--of-organizations-have-e

v. Berg, J., Bonnet, F., & Soares, S. (2020). Working from home: Estimating the worldwide potential. Vox EU-Center for Economic Policy Research. Retrieved from https://voxeu.org/article/working-home-estimating-worldwide-potential#:~:text=Prior%20to%20the%20COVID%2D19%20pandemic%2C%20the%20ILO%20estimates%20that,home%20on%20a%20permanent%20basis.&text=These%20estimates%20are%20based%20on,2019%20or%20latest%20year%20available.

vi. 451 Research-S&P Global Market Intelligence. Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey. June 2020.

vii. Final Report of the National Commission on Terrorist Attacks Upon the United States: Executive Summary. National Commission on Terrorist Attacks Upon the United States. 2004-01-27.

viii. Graham, G. (2009). A Keynote Presentation to the National Emergency Number Association: "Risk Management is No Laughing Matter." Fort Worth, TX.

ix. American National Standards Institute and the Society for Human Resource Management (2020) 'ANSI Standard ASIS/SHRM WPVI.1-2020 AA: Workplace Violence Prevention and Intervention.'

x. FBI (2019). Active Shooter Incidents: Topical One-Pagers. Retrieved from https://www.fbi.gov/file-repository/active-shooter-one-page-summaries-2000-2018.pdf/view

xi. Panchal, N., Kamal, R., Orgera, K., Cox, C., Garfield, R., Hamel, L., Muñana, C. and Chidambaram, P. (2020). The Implications of COVID-19 for Mental Health and Substance Use. Kaiser Family Foundation. Retrieved from https://www.kff.org/coronavirus-COVID-19/issue-brief/the-implications-of-COVID-19-for-mental-health-and-substance-use/

xii. Czeisler M.É., Lane, R.I., Petrosky E., et al. Mental Health, Substance Use, and Suicidal Ideation During the COVID-19 Pandemic — United States, June 24–30, 2020. MMWR Morb Mortal Wkly Rep 2020;69:1049–1057. Retrieved from http://dx.doi.org/10.15585/mmwr.mm6932a1


## Let's Chat

Want to learn more about duty of care for employees working from home? Get in touch or just call us at +1-818-230-9700 to learn more.

# About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to Keep People Safe and Businesses Running™. During public safety threats such as active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 5,200 global customers rely on the company's Critical Event Management Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication devices, and track progress on executing response plans. The company's platform sent over 3.5 billion messages in 2019 and offers the ability to reach over 550 million people in more than 200 countries and territories, including the entire mobile populations on a country-wide scale in Australia, Greece, Iceland, the Netherlands, New Zealand, Peru, Singapore, Sweden, and a number of the largest states in India. The company's critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Public Warning, Crisis Management, Community Engagement™ and Secure Messaging. Everbridge serves 8 of the 10 largest U.S. cities, 9 of the 10 largest U.S.-based investment banks, 47 of the 50 busiest North American airports, 9 of the 10 largest global consulting firms, 8 of the 10 largest global auto makers, all 4 of the largest global accounting firms, 9 of the 10 largest U.S.-based health care providers, and 7 of the 10 largest technology companies in the world. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Abu Dhabi, Beijing, Bangalore, Kolkata, London, Munich, New York, Oslo, Singapore, Stockholm and Tilburg. For more information, visit www.Everbridge.com, read the company blog, and follow on LinkedIn, Twitter, and Facebook.

everbridge®

**VISIT WWW.EVERBRIDGE.COM**

**CALL +1-818-230-9700**