H.E.A.T
Hostile Environment Awareness Training

Building Individual Awareness while Addressing Organizational Resilience

Authors

Michael Blyth, MSc, CSyP, Chief Operating Officer: Risk and Strategic Management, Corp (RSM)

Dr. Donald Bosch, Ph.D., PsyD., Director of Risk Psychology Training: Headington Institute

Chris Williams, Director CARE Security Unit: CARE

Andries Dreyer, Director of Training: World Vision

Aidan Hales, MSc, CSyP, CPP, MSyl, Senior Risk Consultant

Simon Mallett, Director: Risk and Strategic Management, Corp (RSM)
Abstract

Humanitarian aid and development is a multi-billion-dollar sector, representing millions of organizations, with hundreds of millions of employees and volunteers operating worldwide. The community is, by its very nature, drawn towards danger, supporting beneficiaries in high-risk operating areas. In the face of complex global health emergencies, natural disasters and deteriorating security conditions, the imperative for individuals to deploy to, or work in, increasingly fragile and hostile environments commensurately grows. Concurrently, the sector is being held accountable for increasing duty of care expectations from employees, families, donors and governments. Where a perceived or actual failure to appropriately protect people occurs, not only are people physically or psychologically injured, organizations also can face catastrophic litigation and reputational harm. Hostile Environment Awareness Training (HEAT) is part of the duty of care strategy for those working in, or travelling to, high- to extreme-risk environments. It addresses tactical level risks by raising the awareness and competency of the individual in identifying, controlling and reacting to security and safety risks. In doing so, it concurrently reduces enterprise level risks to the organization.

Key Words

Dated: 29th July 2020

For questions on this article please contact: mike.blyth@rsmconsulting.us
**Introduction**

In the last twenty years the humanitarian aid and development community has seen a significant increase in security risks. Concurrently, employees, their families, donors and governments expect an increasing level of sophistication in how organizations protect both people and their financial investment. The sector operates in high-risk, dynamic and remote environments that face heightened human-made and natural threats, and while other organizations typically avoid or withdraw from such environments, humanitarian aid and development organizations actively head towards the danger or maintain missions, despite dramatic changes in the risk environment. Research by Smet, Schreurs and Leysen (2015) (1) indicate that disasters are not only increasing in frequency but are also presenting more complex operating environments, which seem to distress humanity to a considerably higher degree than in the past. As a result, the need for professionalized resilience has grown, enabling organizations to increase or maintain the tempo of operations under deteriorating risk conditions.

Organizational resilience not only addresses the physical protection of employees, it must also ‘de-risk’—as far as is reasonably achievable—all other forms of vulnerability which threaten the survivability of those organizations delivering assistance. Where resilience is weak or absent, the negative implications for the organization, its staff, and the beneficiaries of assistance can be significant. Improving resilience through training not only protects employees from physical or psychological harm, and their organizations from disruptive shocks to operational continuity, it is also necessary to meet the increasing demands of beneficiaries in uncertain and hostile environments (Beal, 2015) (2).

The need to build capacity at the individual level is especially important as the sector prepares to enter a post COVID-19 world (3), where security risks may be more pronounced, and where economic hardships and the absence of humanitarian aid may have undermined societal stability, while providing a vacuum in which criminals and terrorists can prosper.
Research Aims and Methodology

This paper is part of a larger study on organizational resilience in the humanitarian aid and development sector, focusing on the importance of using immersive learning ¹ to develop personal safety, security and emergency management competencies. The aim is to provide security professionals and executive leaders with the information needed to determine what training is required, and the frequency with which training should be conducted. Critically, this paper is designed to help security professionals articulate to executive decision-makers and donors the importance of making resources and funding available to address risk at the individual level. The research seeks to offer action-based outcomes, helping to justify, prioritize and articulate the value of immersive learning techniques. The research draws from a literature review of the security risks the sector is facing, and is augmented by an online survey of 77 senior security professionals, a competency framework focus group of 10 senior security professionals, and a semi-structured interview pool of 32² sectoral risk professionals.

What is ‘HEAT’?

The meaning of the term ‘HEAT’ is highly subjective and open to widely differing interpretations of what constitutes danger and risk management. It is driven by individual knowledge and experience and is complicated by the nuanced interplay of risks across diverse geographies and cultures. The sector has yet to reach a universally-agreed-upon definition of what HEAT means, beyond that of preparing individuals to face an unusual level of personal risk. Presently debate exists within security professionals over six main areas:

1. Content. What competencies are required: what associated knowledge and skills need to be taught, exercised and tested within a program of instruction?
2. Delivery. What methodology is used to deliver knowledge: classroom-based, tabletop exercising, discussion groups, practical sessions / exercising, eLearning or videogames?
3. Duration. How much time is required to adequately teach, exercise and test the knowledge and skills being delivered?
4. Intensity. How realistic and immersive does the learning experience need to be, and what resources are required to produce the required outcomes?
5. Testing. Is the course a pass or fail experience? What are the testing criteria, and what implications exist for the individual and organization if they fail?
6. Frequency. What is the optimal learning cycle for training and refresher training?

A seventh point of debate also exists over who should attend a HEAT course, with dispute focused on whether both international and host nation staff warrant training, and at what risk point attendance should be mandated.

While ambiguity exists over the meaning of HEAT and the knowledge and skills it should offer trainees, there is general agreement that learning should, ideally, be delivered through an

---

¹ Immersive learning allows an individual, or group, to apply knowledge to a practical problem, and so learn by doing.
² Pseudonyms have been used for anonymous attributes, unless the organization they work for is specified; then fully attributed references are provided.
Hostile Environment Awareness Training
Building Individual Awareness while Addressing Organizational Resilience

immersive experience in order to contextualize the meaning of knowledge, while concurrently
developing ‘muscle memory’ within simulated high-stress conditions. HEAT should vaccinate
individuals against debilitating stress during unusual emergency situations. Presently, courses
run from one to five days in duration, resulting in significant variances in content, delivery, and
duration. The intensity is also inconsistent, with some educational strategies including varying
degrees of stress for participants (including reaction to gunfire, explosions and simulated
torture), while others argue that stress results in a negative learning experience and must be
avoided.

Attendees are rarely, if ever, ‘failed’, even if they do not absorb or apply the knowledge
provided successfully, or where they show signs of making poor—and potentially life-
threatening—decisions under stress. Where organizations self-run training, more latitude to fail
participants exists as the metric for a ‘pass’ can be agreed between key decision-makers. A
‘pass mark’ may include technical knowledge and its application, the participant’s attitude, or
how well—or badly—they respond to stress. That said, where a fail-point is determined, then
significant risk exists: a decision may be disputed, can be difficult to substantiate, and may
cause personal or employment harm to the individual. As such, the Security Department must
work in partnership with Human Resources and Legal to ensure that no ambiguity exists over
performance expectations. Commercial companies are in a different position, in that they are
not empowered to fail a participant, unless specifically mandated by the sending organization.
Where organizations do require a ‘pass or fail’ determination, then commercial trainers run the
risk of being poorly graded by disgruntled participants.

Training methodology differences between organizations who self-run training, and those who
provide it as a commercial offering, can also exist. Self-hosted training may focus more on
practical outcomes, while a commercial company may be motivated to seek a balance between
both value and enjoyment; effective but ‘boring’ training can result in weaker participant
evaluations, thus dampening future business. As such, the ‘Hollywood Effect’ comes into play
more so for commercial companies who need to motivate participation, compared to self-
hosting organizations, which can mandate attendance. Commercial companies are heavily
influenced by profit, moving between investing heavily to generate a strong ‘brand’ and so
providing more client engagement, to streamlining investments to maximize profitability if the
brand factor is less important. Where commercial companies seek to create a brand, then
(arginably) training will be more richly resourced, especially where investments are then
leveraged across multiple clients, or are capitalized across multiple organizations and time.
Where training is self-run, then investment is more typically applied to a single organization
(with exceptions), and so resourcing levels are more fixed.

Psychological risk management is also a growing factor where HEAT moves within the grey
zone of positive ‘stress’ and negative ‘distress’. Participants bring different experiences to
HEAT, with some learning experiences triggering emotional distress, as memories and
experiences are relived. Psychological screening and monitoring can be a requirement for self-
run courses, albeit with challenges, as individuals may not volunteer traumatic experience
information before, during or after a course. Psychological experts also come with a high—
albeit warranted—price tag, driving up the cost of training. For commercial companies experts
within the field of post-traumatic stress disorder and counselling can be included; however, the
sending organization(s) must drive the requirement for screening and monitoring and must
manage post- course counselling support. Regardless of the level of psychological expertise
applied to HEAT, it is inescapable that any immersive learning experience must include very careful consideration of the mental wellbeing of attendees, and must be maturely configured to ensure positive—not damaging—learning outcomes. Bill, who has held multiple Global Director of Security positions for some of the largest NGOs, stressed the need for well-designed and sensitively constructed training:

I remain continually concerned about immersive training that does not take into account the psychological triggers for those participants who may have already had experiences in their life that are traumatic.

Where sectoral standards are sought, security and training professionals must determine the balance between: 1) technical content, 2) the ratio of theory to practical learning, 3) the manner in which immersive exercising occurs, 4) how much time is allocated to learning, and 5) the right level of ‘stress’ to simulate realistic scenarios. Large and well-funded organizations are more likely able to support longer, higher-cost and more resource-intensive training, while others may only be able to fund or engage in succinct, low-cost and resource-lite courses. This suggests that ‘HEAT’ should be an umbrella term which sits atop a number of levels. Scalability is required, giving organizations the flexibility to move between bronze to gold standards, based on two core factors: 1) a security risk assessment of what level of knowledge and experience is required to address the individual’s personal risks, and 2) an economic assessment of what is financially achievable. No one standard can be applied within such a diverse sector, outside of thematic areas of content, the inclusion of a blended learning approach, and the application of appropriate stress levels.

The risk of a layered HEAT methodology is that learning may become a ‘tick in the box’ exercise, focusing on economic savings verses learning value. Ideally, the Security Risk Assessment (SRA) should outweigh the cost factor, with executive leaders being willing to invest in their people appropriately. Transferable knowledge must also be effectively evaluated to enable organizations to measure learning experiences gained from other organizations or commercial providers, or where government or military training programs—such as SERE training—may cover some or all of the learning requirements. Informed decision-making is required when determining what constitutes applicable learning. For example, an experience learnt in the military where the individual was armed, part of a well-trained military unit, and where substantial resources were available, in no way reflects the reality of the humanitarian world.

Findings from the interview pool suggested that some decision-makers seek content and course duration ambiguity within HEAT courses, to reduce organizational accountability. If a standard is hard-coded into a course, then any failure to meet these standards—every time—exposes the organization to legal and reputational risk. This presents a potential clash between the security professional seeking to protect the individual, and the Legal Department, seeking to safeguard the organization from tort lawsuits. From a legal and reputational standpoint, those organizations who self-run HEAT are also directly accountable for the standards developed, and so assume full liability for any hostile scrutiny following an incident. Conversely, where commercial providers are used, then ‘arms-length distance’ liability protection can, arguably, be

---

3 SERE: Survival, Evasion, Resistance and Escape
4 This does not reflect the opinion or statements of the authors
Hostile Environment Awareness Training
Building Individual Awareness while Addressing Organizational Resilience

provided to the organization. Resultingly, HEAT means different things to different people, with Brad, the head of training for a large NGO, offering that:

The word HEAT shouldn't exist in my opinion at all... it is all over the place, and it needs to be standardized.

From a government perspective, HEAT also has different meanings, with USAID (4) offering the following thematic training areas for high risk areas: 1) situational awareness, 2) personal security, 3) crisis and hostage management, 4) defensive driving, 5) first aid; and 6) carjacking risk awareness. The United Nations SSAFE (5) program covers many of the same areas, including: 1) working in field environments, 2) managing injuries in field environments, 3) communications and technology, 4) coping with captivity and detention, and 5) vehicles and movement.

The following list of relevant HEAT topics was drawn from the interview pool:

- Personal security techniques
- Tactical risk assessments
- Kidnap and ransom awareness
- Civil disorder awareness
- Active shooter and armed aggressors
- Remote casualty stabilization
- Indirect and direct fire [SAF] attacks
- PTSD awareness
- Basic self-defense
- Information security awareness
- Communicating under duress
- Cultural awareness
- Criminal threats and responses
- Hotel and guesthouse security
- LGBTQIA risk awareness
- Gender security risks
- UXO, IED and mine awareness
- Anti-carjacking techniques
- De-escalation techniques
- Legal and illegal checkpoints
- Emergency equipment and ‘Grab Bags’
- Trip planning and risk avoidance

Regardless of the duration or curriculum, a HEAT course seeks to build the resilience of the participants, enabling them to effectively address personal and group risks — reacting quickly,
effectively and with a higher degree of assurance to life-threatening emergency situations. The objective is to reduce the debilitating effects of uncertainty and shock when faced with a high-stress and fast-moving threat for the first time, through the blending of classroom-based instruction and exposure to simulated situations that promote practical problem-solving skills. Scenario-based learning helps the individual to overcome disbelief which can cause a dangerous delay between identifying a threat and reacting to it. HEAT also offers individuals with pre-formed problem-solving ‘options’ to select from when faced with predicted threat situations. This is especially important, as stress and fear can result in the release of cortisol which interferes with complex thinking, making people faster, stronger, yes, but while also interfering with cognitive functioning—reasoning and rational decision-making. Emotions can also trump reason, placing people at heightened risk where survival instincts diminish, or replace, rational thinking.

Ideally a competency framework for HEAT would be aligned to an SRA approach, allowing organizations to select from a sliding scale of HEAT variants which meet different technical content needs, the right ratio of theory and practical training, and the appropriate level of immersive learning intensity. This would then drive the duration, realism and intensity of training, and the associated level of financial investment.

The Value of Immersive Learning

Research by Kowalski and Vaught (2020)\(^6\) has shown that when faced with a unique and stressful situation, people may revert to familiar activities, rather than a new and complex act which might in fact save their lives, with intuitive overtaking analytical judgement. Ripley’s
crisis and disaster case studies offer real-world examples of how inoculation to high-stress situations enhances an individual’s probability of survival. Under crisis situations, there is often limited information to guide effective decision-making, and stress narrows the focus of attention while impacting behavior. Importantly, this results in a sense of uncertainty which automatically engages the more primitive survival structures of the brain, reducing the ability to think clearly. By running through simulated conditions, people are more likely to move through the stages of belief, deliberation and action more quickly and effectively. They will more likely recognize the effects that stress has upon them as an individual—having experienced it before—and will be more likely to prioritize effective courses of action to address real, rather than perceived, threats. Bosch (The Headington Institute, 2015) studied the value of immersive or ‘high-fidelity’ learning, recognizing that experiential learning is vital:

This model follows the principles of high-fidelity stress exposure training and has been empirically shown to be the best method by which to teach the kind of preparedness and skill needed to operate in high intensity situations. Through the integration of psychological and security training, with practice in highly realistic scenarios, these humanitarian organizations best prepare employees deploying to high risk environments to not only avoid but also to survive a hostile security event should it occur.

David, the head of risk management for a US NGO, supported the Headington Institute’s findings, indicating that anyone travelling to a high-risk environment would be required to attend a HEAT course:

I proposed to my President just yesterday, actually, that I wanted anyone traveling on assignment to go through a three-day HEAT training course, period. It should be required, end of story.

Adults learn through three domains: 1) the cognitive, which includes lectures, brainstorms and discussions, 2) the affective, which addresses value clarification exercises, nominal group processes and consensus-seeking activities (emotion), and 3) the behavioral, which includes roleplays, simulations and teach-backs (NHI, 2020). The delivery of knowledge is then imparted through visual, auditory and kinesthetic means, as shown in Figure 1.

HEAT provides the mechanism to include all three learning systems, while allowing for both an individual and group learning experience against a wide range of different threat scenarios which is meaningful and so has value to the individual, as well as the group. Narli’s (2010) study of constructivist learning underpins the value of active learning, the process through which learners carry out learning on their own, and where they are required to proactively think about their learning experience and what it means to them. Once knowledge is learned, then it must be maintained. Chi et al., offer that retention rates are typically: reading 10%; seeing 20%; hearing 30%; seeing and hearing 50%; collaboration 70%, and doing 80% (1989, p. 13). HEAT incorporates all forms of learning, and given it is a practical life-saving skill, requires an appropriate emphasis on ‘doing’ in order to be effective.
Immune learning, through HEAT at the individual level, or through emergency or crisis management exercises at the leadership level, provides the environment where learners develop and apply knowledge and skills on their own, or within a group of peers. It offers the framework where the individual must actively think about how their knowledge addresses real-world threats. The traditional teaching approach, where learners are passive information receivers, creates an environment where learning is not optimally received and retained, and where the opportunity to apply knowledge is either limited or absent. Narli offers that: ‘some educational psychologists say that students from different parts of the world learn better when they gain experience together and tackle problems which require authenticity and simulation’ (2010, p. 37). This is supported by Craik and Lockhart’s (1972) concept on the ‘level of processing’ which states that familiar and meaningful stimuli is better retained than less meaningful stimuli. Accordingly, HEAT must be realistic and relevant in order to resonate with the learner, being viewed as meaningful and of practical value.

Knowledge retention and knowledge transfer are different (Semb and Ellis, 1994). The ability to recall pieces of knowledge does not constitute the ability to apply them effectively to a real-life situation. As such, learning requires both the ability to retain technical knowledge or practically taught skills, and then to apply this information effectively against the context of different, and often high-stress, situations. Effective HEAT provides knowledge, and then requires the individual to apply it to a real-life and high-stress situation. This immersive learning process accelerates knowledge growth, while at the same time amplifying its relevance to the participant. The value of instruction—and the return of investment to the employer—is therefore extended past the typical point where refresher training is required.

The goal of HEAT, then, is teaching the individual about a series of risks, before exercising the application of the newly-acquired knowledge and skills, and, in its most complete form, testing them through realistic, simulated situations. HEAT can include all forms of learning, through a blended experience, utilizing classroom training, discussion exercises, tabletops, practical sessions and practical or scenario-based exercising. The true value of HEAT is the immersive component, the application of knowledge and skills against a stressful and fast-moving series of challenges which the individual, or group, must overcome. Peter Sjøstedt (Global Safety

---

Figure 1: NTL Institute - Applied Behavioral Science Learning Pyramid
Training Coordinator: Danish Refugee Council) offered that HEAT built individual resilience against safety and security challenges, stating that:

People will actually be able to independently take responsibility for their own safety. They can proactively do what’s needed to avoid getting into trouble, or at least minimize the risk. They have the skills, knowledge and competency to solve problems, once they arise.

The curriculum of a HEAT program should logically reflect the probable risks the individual may face, from low probability and high-impact threats such as a kidnapping, to a high probability and low to medium threats such as a mugging or natural disaster. Kravitz and O’Molloy (15) posit that: ‘In many cases, simple training can go a long way to avoiding serious injury or death’ (2014, p.6) and HEAT plays a key role in meeting the increasingly risks employees face when working in areas subject to higher levels of crime, social instability, victimization5, terrorism or war.

HEAT not only offers value to the individual, it also offers a mechanism for transformative change where organizations can avoid, reduce or manage security challenges at the point of incident occurrence by empowering staff through knowledge and practice. HEAT also builds a community of risk practitioners in the organization, rationalizing the value of security risk management vertically, from the most junior member of staff to the executive leadership team, and laterally across functions, geographies and cultures. The value of HEAT then extends beyond the obvious, including raising the profile and value of the security community within the organization, as well as the wider sector—while also contributing to the broader resilience strategy.

HEAT and Duty of Care

Duty of care is a cornerstone of resilience, demonstrating the ethical and professional investment taken to protect the physical and psychological wellbeing of people. However, duty of care is not just about protecting people; it is also about protecting the organization from disruptive incidents —specifically from litigation and reputational harm. Duty of care includes two key elements, action and evidence. Not only is the organization required to do the right thing, they must also be able to prove it after the fact. The ability to evidence appropriate security steps to protect the individual enables organizations to demonstrate to employees, their families and to donors a professional approach to risk management. Guttry et al (16) noted that: ‘for international organizations, reputation plays an important role particularly in terms of legitimacy and credibility. When strong allegations of misconduct or failure to meet high duty of care standards are directed towards international organizations their legitimacy and credibility is put under risk, undermining the organization’s effectiveness’ (2018, p. 23).

Duty of care expectations have evolved over the past two decades and now demand that humanitarian aid and development organizations meet the same standards as their commercial counterparts, with Bickley (17) observing that: ‘the duty of care benchmark has risen significantly over the past decade, and what once was considered good enough would certainly not be considered adequate today’ (2017, p.8). HEAT forms an important part of duty of care

5 Notably for women and members of the LGBTQIA community.
requirements, with organizations increasingly being required to invest into immersive training, with Andy, a Regional Security Director for a major humanitarian organization, stating that:

I think situational awareness is a big word at the moment, that and duty of care. Situational awareness goes into training so developing trainings like online trainings and going into the physical training side is now being implemented across the board. You have to do some sort of awareness training. At a medium risk, you'll have to do a more advanced training. When you go into the hostile and high-risk areas, you're having to do a physical Hostile Environment Awareness Training.

Figure 2 represents 77 seasoned security professionals’ opinion when asked to respond to: ‘Organizations place great importance on building the knowledge, skill and confidence of the broader staff population in risk management at a personal level.’ Of the survey participants, only 43% felt that organizations saw positive value in addressing individual safety and security risks through training. This result is complicated, as the humanitarian population is broadly split between three main groups: 1) headquarters staff, who are office-based, 2) international travelers and 3) host nation staff, who reside and work in their home country. The last category of staff represents the largest portion of the humanitarian community, and those who typically face the most persistent levels of personal risk. However, litigation and reputational risks are more commonly found where an individual travelling internationally for business is harmed through a security incident.

The results indicate that while security risks to the individual are evident, the sector has yet to fully embrace the need and value of HEAT. Camila, a senior risk leader at the headquarters level, supported the view that individuals working together to resolve realistic problems within a HEAT course was beneficial in developing competency at the personal level, stating that:

From a duty of care, wanting the staff to be fully prepared, I think they should receive some sort of in-person and immersive training.

Over the past decade, the importance of HEAT has grown in prominence, as international staff increasingly demand immersive training before deploying to high-risk and unfamiliar environments. Host nation staff are similarly demanding some form of HEAT, as they recognize they face prolonged exposure to many of the same risks, even though working within their home country. Host nation staff also form the largest portion of the learning population.
Jackson and Zyck (18) note that the value of training has seen a marked increase, stating that: ‘in 2011 only 26 percent of local NGO staff reported receiving security training, while that figure was 47 percent in the latest (2015-2016) survey’ (2016, p. 55). This report resonates with the findings in Figure 2, which indicates 43% of organizations surveyed now actively support individual level security awareness training. It is unclear whether the catalyst for change is organizations recognizing and embracing the benefits of HEAT, or whether they have been forced to adopt this training to address external pressure. Debate also exists as to whether national staff warrant the same degree of training as those traveling to unfamiliar operating environments, where they might ‘stand out’ and lack a family and social support network, with cost and the availability of training resources leading to a greater focus on the international traveler.

A large number of studies, as illustrated in Table 1, have been conducted on the physical risks facing employees and volunteers within the sector, removing any ambiguity over the increasing probability that people will be exposed to, and be harmed from, security risks. Stoddard, Haver and Czwarno (19) state that: ‘INGOs seem to be taking on greater risks than ever before’ (2016, p. 5), suggesting that the frequency and severity of security incidents, and subsequently risks, will only increase (with spikes occurring) over time.

![Table 1: From Aid Worker Security Database (2020)](image)

The cascading effects from a security incident often exacerbate the disruptive impacts to the organization and confuse risk control measures. The secondary and tertiary risk implications originating from the initial incident are often more likely to cause strategic and lasting harm than the initial incident. These can also quickly deplete organizational capacity and resources, while overwhelming ill-defined and unpracticed resistance measures (Maren, 1997) (20). Where risks are ‘known,’ they must be appropriately treated, with Guttry et al. stating that: ‘duty of care constitutes a non-waivable duty on the part of organizations to mitigate or otherwise address foreseeable risks that may harm or injure its personnel and their eligible family members’ (2018, p. vii-viii). They go onto say that duty of care addresses incidents of physical harm during the performance of work, and a violation is proved by: ‘demonstrating the lack of measures adopted by the sending organization to secure and guarantee the safety of personnel working on the ground’ (p. 5).
Legally, organizations are required to articulate risks, and to train people to address them. Lockton (21) the world’s largest privately held insurance brokerage firm, states that: ‘organizations have legal obligations to act towards others and the public in a prudent and cautious manner to avoid the risk of reasonable foreseeable injury to others’. Kemp and Merkelbach (22) define the requirement from both an ethical and legal standpoint: ‘safety and security are not only an ethical and moral concern but a legal obligation’ (2011, p. 4), and extend the obligation beyond employees and onto seconded staff where the court found in the 24th October 2007 Karachi litigation case that: ‘even if the employer entrusted his employees’ safety to a third party, he still has a duty of care towards them and has to check that the safety measures taken were complied with’ (p. 33). Where duty of care standards are not met, then both the individual and the employer suffers. Erik, a humanitarian legal expert, supported the need for the ‘see, hear and do’ approach, but indicated that the level of investment and the degree of professional delivery for immersive training was inconsistent across the sector:

I see some organizations that are extremely sophisticated and put a lot of time and effort into this, and I see others that, either because they’re naive or they don't feel like they have the resources, have actually put very little effort into it.

Kemp and Merkelbach reinforce the negative consequences of not meeting appropriate duty of care requirements, stating that: ‘The consequences of legal liability to International Aid Organizations can be expensive not only financially, in terms of damages that may be payable to staff following litigation, but also in terms of potential criminal liability, loss of reputation, damage to public relations, adverse effects on staff morale and recruitment and compromising fundraising efforts’ (2011, p. 26). While universal agreement on the need for HEAT may be absent, sufficient recognition of its important is certainly present.

Guttry et al. (2018) explore—in depth—the duty of care requirements associated with multiple agencies as it relates to HEAT or similar courses, noting that the United Nations recognize the importance of providing its staff and their dependents security relevant information, including both online and face-to-face security trainings, with up to a 5-day HEAT program (Safe and Secure Approaches in Field Environments (SSSAFE)) for those working in higher threat environments. A similar model is used by the World Bank Group (WBG), the International Monetary Fund (IMF), the African Union (AU) and the Organization for Security and Co-operation in Europe (OSCE). All require appropriate training to be provided to staff, and, at times, their dependents. The USAID Office of Foreign Disaster Assistance (OFDA) Safety and Security Sector Update report (23) also recognizes the risks individuals face, stating that: ‘Delivering humanitarian assistance to vulnerable populations around the world often requires relief organizations to operate in insecure environments, putting non-governmental organization NGO staff at risk of death, injury, or kidnapping’ (2018, p .2), with OFDA providing a HEAT variant course for NGOs.

This level of recognition forms a benchmarking standard against which the community should—and may eventually be required to—align itself. The norm of requiring HEAT will also be driven by the increasingly numbers of organizations who embrace HEAT, and so establish a sectoral standard against which all organizations will ultimately be held accountable.
Defining the Frequency of HEAT Refresher Training

The optimal frequency for HEAT refresher or recertification training is ill-defined within the sector, as no studies have been conducted to determine how long knowledge is retained through immersive learning. Initial studies by Ebbinghaus in 1880 \(^{(24)}\) on memory retention that coined the ‘Forgetting Curve’ have been replicated by Murre and Dros in their study *Replication and Analysis of Ebbinghaus Forgetting Curve* (2014) \(^{(25)}\). These studies indicate that certain styles of learning have associated retention patterns, with retention studies ranging from 3 days to 120 days. While research has produced uneven results, all uniformly agree that people forget, and that significant memory fade occurs over a period of 100+ days. Resultingly, unless knowledge is consistently applied through action, and in a manner that resonates through perceived or proven value to the learner, it is unlikely to be retained. Consequently, critical life-saving knowledge is quickly lost.

The challenge facing the sector is determining how often organizations should reinforce learning. While the optimal frequency for refresher training has yet to be formally defined, most organizations running HEAT or equivalent programs agree that skill fade occurs between 3 to 5 years, with Table 2 showing the certification validity for major organizations running internal HEAT programs. It is important to note that, while refresher training goals may be at the 3rd or 5th year point, cost and logistical challenges (including international travel and social distancing restrictions resulting from COVID-19) can hamper the ability to implement this training cycle. Where refresher training is not conducted, then the individual becomes less effective at recalling and applying knowledge, and the organizational exposure to litigation and reputational risk is exacerbated. The United Nations has affixed no defined refresher point; however, at the local level, refresher training does occur, being driven by a host of local factors. Other organizations like the WBG and IMF refresh knowledge through eLearning and videogame solutions, rather than requiring participants to physically return to a training center for the in-person learning experience.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Certification Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Care International</td>
<td>5 years</td>
</tr>
<tr>
<td>United Nations</td>
<td>Open</td>
</tr>
<tr>
<td>World Bank Group</td>
<td>3 years</td>
</tr>
<tr>
<td>Danish Refugee Council</td>
<td>3 years</td>
</tr>
<tr>
<td>Norwegian Refugee Council</td>
<td>3 years</td>
</tr>
<tr>
<td>International Monetary Fund</td>
<td>3 years</td>
</tr>
<tr>
<td>World Vision</td>
<td>5 years</td>
</tr>
</tbody>
</table>

*Table 2: HEAT refresher frequency*

The Problems Associated with HEAT

Research has identified three main challenges for organizations in terms of: 1) understanding or evidencing the value of immersive learning, 2) funding training and 3) identifying venues and credible providers. Any one of these challenges can derail the organization’s approach to providing personal safety and security training that delivers powerful and long-lived learning outcomes, resulting in either a sporadic and disjointed approach … or no approach at all.
Hostile Environment Awareness Training
Building Individual Awareness while Addressing Organizational Resilience

The ease of justifying an investment of money and time into training—and allowing individuals to step away from their role and travel at considerable expense to attend training—can be a significant challenge for the security professional. To effectively argue the case, qualitative and quantitative data is required to ‘prove’ value. An evidenced approach requires two test groups operating in the same area. The group must represent a defined demographic and must perform similar tasks over a longitudinal study period in order for results to be meaningfully evaluated.

One test group must be provided risk mitigation controls to address defined threats; the other should be denied these resources, and so face the environment without the ability to control risks. This creates legal and ethical challenges, as the acknowledgment of a threat dictates the need to prevent harm. Any failure to address a vulnerability is both immoral and presents potential litigation and reputational harm, if a breach of duty of care can be asserted where an organization acted or failed to take action (in respect to a threat) if the action or failure to act was: negligent, voluntary or had foreseeable and natural harmful consequences.

The challenge, then, is for security professionals to show why an investment in this form of training is beneficial, and how it should be prioritized against competing organizational demands. Gavin, a well-established academic and renowned author on security risks in the sector, indicated that, while driver risk reduction data was more readily available, no formal studies had yet been conducted on the value of HEAT courses:

Training is a very interesting area, and we have long thought about doing a study on the impacts of training for an organization’s ability to manage security risk and achieve secure access in challenging areas. Anecdotally you hear all the time about certain training inputs such as defensive driving techniques and how they have saved lives, and people who have undergone HEAT say mixed things about how it helped them in extreme situations, but there isn’t any hard evidence which can be shared.

Most of those interviewed stated that they could readily cite anecdotal evidence where such immersive learning had been useful, including practically dealing with a security incident and then psychologically recovering from it—but that there was a lack of hard statistical data to reinforce their perception that immersive training was beneficial. In rare instances, anecdotal or retrospective studies have been conducted; however, these results are rarely published. Andries Dreyer (Director of Training for World Vision), indicated that his organization had conducted a formal study into the benefits of HEAT, offering that:

We have been training HEAT’s for many years and have extensive data and overwhelming staff feedback that show that the return on investment on HEAT is more than justified. In conjunction with the Fuller Graduate School of Psychology and the Headington Institute we surveyed HEAT graduates from the past five years of training. Key findings indicate that fully 97% of those who responded indicated that HEAT increased their awareness of security as well as helped them feel more prepared to face a security incident. An even more compelling finding indicated that 58% of graduates had experienced a critical incident following HEAT and that 98% of these indicated that the training had helped them understand and manage their own responses during the incident, thereby improving their chances of survival. These solid statistics support our training model of pairing security and psychology and should influence those who doubt the validity of what the training is designed to do.
Hostile Environment Awareness Training

Building Individual Awareness while Addressing Organizational Resilience

Where organizations have not suffered through a crisis, the security professional can face an uphill battle, with decision-makers exhibiting a range of responses, including disinterest, disbelief or outright opposition. Where opposition exists, the professional is often faced with passive aggressive challenges, being required to find statistical proof of the empirical value of immersive learning. Absent research and the resulting hard data upon which value can be measured thus presents a ‘Schrodinger’s Cat’ scenario where the professional is required to prove what may or may not happen… if an action is or is not taken. Alternatively, leaders may present such unreasonable and changing evidentiary demands on the professional that their energy is depleted, or their bandwidth is insufficient to sustain the argument.

Where quantitative data is available, this typically represents the number of incidents that have occurred, rather than the number of incidents that may have been prevented. The challenge is that proof that danger exists does not always show how effective risk controls will be. A further complicating factor is where datasets are limited; then, meaningful trend analysis ranges from problematic to impossible. Where defined risk controls are enacted, and a longitudinal study is run, then pre-control data can be measured against post-control results to show the effectiveness of risk prevention or reduction measures. This, then, evidences how risk control measures protect people, and reduce insurance costs, or business losses.

The ability to fund security training (if it is not funded by donors), can place a financial strain on organizations, especially those who have not included the cost of training into a program budget from the outset. Where security funds are absent or limited, or where the funding mechanism prevents or hinders recovering training costs, then organizations are forced to fund training from available fee and overhead budgets. Historically, organizations have been reticent to include security costs in budgets, for fear of increasing a proposal cost, and so reduce the win potential. Concern is also associated with how security costs are perceived within the donor evaluation process. While donor reticence to fund security may have been true in the past, increasingly donors recognize the value of such training, and are willing to fund it. The ECHO report (27) indicates that: ‘Most major donors are willing to fund security measures and training’ (2004, p.4), indicating that despite donor willingness to support HEAT, many organizations cite a lack of funding as a rationale for failing to train their staff.

USAID includes the provision for pre-deployment training within some contracts, citing that any costs below the ‘small purchase’ threshold do not require Contracting Officer approval, so long as sufficient funds have been included within the budget. Bickley also notes that where organizations recognize the need for HEAT, the cost of financing training has been a barrier: ‘Many NGOs understand the importance of security training; in practice, however cost and availability remain significant barriers to organizations actually implementing and sustaining security training’ (2017, p. 46). Confusion within the sector remains over whether donors will fund training, despite the clear recognition by many agencies of the value of immersive training. Brabant (28) reinforces the ability for implementing partners to draw on available funding, stating that: ‘the major humanitarian donors are prepared to fund appropriate and justified safety—and security—related expenditures’ (2010, p. 295).

Where organizations see value in training and are willing to commit time, funds and resources (or approach donors for funding), then the next challenge is identifying which resources best support the training requirement. The interview pool had mixed feelings regarding whether sector-specific training was needed, or whether commercial training resources met capacity-
Hostile Environment Awareness Training
Building Individual Awareness while Addressing Organizational Resilience

building needs. Adam, the Global Security Director for a major NGO, indicated that, while appropriate training was widely available, not much had been developed to meet the explicit needs of the sector:

There are courses out there, absolutely. There aren’t so many tailored to humanitarian security, but my experience is that humanitarian security isn’t completely unique, either, so I think people in the sector are learning from other courses that are available.

The challenge of identifying credible training providers and suitable venues for the immersive learning experience can devalue the perceived value of a HEAT program quickly. A poor training experience undermines the credibility of the security professional advocating for immersive learning, while concurrently devaluing the importance of the training itself. Bill stressed the need for well-designed training:

I think really well-designed HEAT training is particularly useful.

Alice, the Global Director of Security for a major NGO, emphasized the need to be able to benchmark against a consistent standard in order to measure the organizational effectiveness in managing increasingly complex risks, stating that:

We need to have a standard. We need to have a benchmark to run to.

The challenge then is to define what constitutes ‘good’ training, where organizations do not have an internal training team to conduct a HEAT course. Even where larger organizations have internal instructional resources, the ability to reflect (impartially) on the curriculum and manner in which training and exercising is conducted requires a standard to benchmark against. The sector must then select a metric for determining what is appropriate and credible training from the options of: 1) training organizations holding 3rd party training center status, 2) programs of instruction which come with independently recognized credentials, 3) training institutions that have both a proven track record in the technical area, and importantly in the sector, 4) a professional review of the curriculum and manner in which training is delivered and 5) past performance feedback from peers within the sector who have participated in training and can validate its excellence.

Where organizations outsource HEAT, they are required to develop their own evaluation metrics, without the benefit of a standard to align to, in order to sift the wheat from the chaff. Donna, the Global Director of Security for a large NGO, indicated that good providers do exist, and so resources are readily available to support HEAT programs:

I think there's a lot of good courses out there that people can opt to take to give them an awareness of the security situation that they're going to be going into.

The production of knowledge strategy is currently ill-defined, but nonetheless forms the cornerstone of what should be in a HEAT curriculum. Etienne Wenger (1999) (29) observed that people are social beings, and this is true of the security community in terms of how training standards are developed, and how knowledge is applied. Ethnography also plays a role, as subset cultures exist within the sector, presenting different belief systems that influence how knowledge is both formed, delivered and received. This is important in how curriculums are designed and implemented. To be both credible and effective, professionals with the different skill sets for instructional design and training implementation are required, drawing from
Hostile Environment Awareness Training  
Building Individual Awareness while Addressing Organizational Resilience

experts with a credible background, experience, credentials, and competencies. Where possible, training design should be aligned to recognized 3rd party standards to enhance performance, and evidence competency. These may include recognition as an Approved Training Center through the Institute of Leadership Management, through externally accredited quality assurance programs, such as the City and Guilds Assured program, or by aligning training against the upcoming ISO 31030 standards for Risk Management—Managing Travel Risks (with an anticipated release in 2021).

Where the curriculum and instructor team are effective, then the next challenge the sector faces is finding the right venue and training resources. Training providers also face the risk of unwanted attention, or arrest, when seeking to run HEAT within some countries, with INSO trainers being arrested in Kenya (2015) for possessing wooden replica weapons in training. Peter Sjøstedt (Global Safety Training Coordinator: Danish Refugee Council) noted that finding the appropriate training venue, with supporting resources, was a major challenge:

> It can be difficult to find places where we can actually do that kind of training, because certain governments and authorities will not allow that kind of training.

Training venues require appropriately large parcels of real estate to allow for realistic scenario-based learning to be conducted. They require the necessary infrastructure to provide the backdrop against which knowledge can be taught, and within which exercising can be conducted. The facility must have the ability to employ realistic effects to support learning, including the use of simulated explosives and gunfire. Ideally, the venue should be discreet and offer a ‘single-site’ user service, avoiding the distraction of other courses being run at the same time, as humanitarians are unlikely to be inclined to train alongside foreign military units or private military contractors; the realism of a scenario will be quickly diluted as neighboring training compromises the flow and realism of the learning experience. Training in proximity to government forces can also conflict with the ethos of many organizations, requiring them to seek alternative venues.

RSM HEAT ‘Pandora’ Training Centre: Bullet Penetration Training Aids
Few, if any, humanitarian aid and development organizations, or even institutional development bodies, can self-fund and operate a suitable training venue that covers 90+ acres, is appropriately licensed, and which holds an armory of live weapons, explosive simulators, inert explosive devices, and unexploded ordnance. The costs are prohibitive, and the logistics and administration burden can be overwhelming. The approval process through local government can also be lengthy, exhausting and economically risky, with parts of the local community being hostile—often due to a lack of understanding—to such training. Rather, organizations must piggyback on military installations, or must identify suitable commercial training venues that offer the right setting, privacy, training aids and attentiveness to meet learning goals. Retaining a dedicated training team can also be costly, unless the through flow of participants is sufficiently high, and so only the largest and best-funded organizations can afford to self-administer training.

Conclusion

Research across multiple fields of study supports the value of immersive learning in addressing increasing levels of security challenges facing the sector. The evolving complexity of risk, duty of care expectations from staff, families, donors and governments, combined with escalations in natural disasters, crime, social instability, hostile government targeting and terrorism, all underpin the increasing importance of adequately preparing people to face fast-moving and high-threat personal risks. Immersive learning enables participants to absorb, make use of, and retain knowledge. It is the most effective mechanism for instilling life-saving knowledge and skills which not only protects people, but also protects their employer. A single instance of avoiding a crisis could, arguably, offset the associated business and operational disruptions, as well as the direct harm resulting from litigation and reputational damages. Currently, only the largest organizations run in-house immersive training courses, with the majority leveraging the rare commercial training provider who offers the appropriate curriculum, instructors, resources and real estate needed to meet immersive learning needs. Both groups face the same challenges: validating what knowledge should be taught, developing common syllabi, delivering knowledge effectively, and evidencing the utility of the training.

The necessity of moving the agenda of effective training forward to a scalable standard must be both developed, and recognized, across the sector in order to meet the needs of both the micro and macro organization. These standards will not only shape the curriculum and manner in which knowledge is imparted, practiced and tested, they will also form the metric by which to evaluate internal training resources or commercial provider excellence. Concurrent to this, a longitudinal study should be conducted to determine what competency framework should be applied to HEAT variants, as well as to measure where immersive learning demonstrates value to both individuals and their organizations. These, then, can be presented internally to organizational decision-makers, as well as externally to donors, thereby evidencing the importance of investing in high-fidelity training.

Acronyms

SAF: Small Arms Fire.
PTSD: Post-Traumatic Stress Disorder.
LGBTQIA: Lesbian, Gay, Bi-sexual, Transsexual, Queer, Intersexual, Asexual.
UXO: Unexploded Ordnance.
IED: Improvised Explosive Devices.

References


