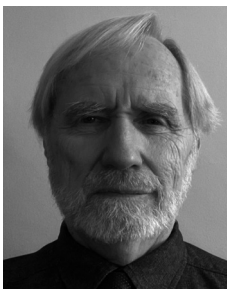
Michael Blyth



Donald S. Bosch

Chris Williams

Hostile environment awareness training: Building individual awareness while addressing organisational resilience

Received (in revised form): 26th November, 2020

Michael Blyth*

Chief Operating Officer, Risk and Strategic Management, USA

Donald S. Bosch**

Clinical Psychologist, Humanitarian Psychological Services, USA

Chris Williams†

Director CARE Security Unit, CARE, USA

Andries Dreyer†

Director of Training, World Vision, USA

Aidan Hales‡

Senior Risk Consultant, USA

Simon Mallett‡‡

Head of Risk Consulting and Operations, Risk and Strategic Management, USA

***Mike Blyth** is the Chief Operating Officer for Risk and Strategic Management Corporation. He is an ISO certified Lead Auditor for business continuity management with diverse commercial and military experience. He holds a master's degree in security management from the University of Loughborough and is currently studying for a doctorate in security and risk management at the University of Portsmouth. His books 'Security and Risk Management: Protecting People and Sites Worldwide' and 'Business Continuity Management: Building the Incident Management Plan' are published by Wiley.*

***Don Bosch** is a licensed clinical psychologist and psychoanalyst, holding doctoral degrees in both disciplines. He has worked extensively in the humanitarian field with global rapid response teams and individual aid workers. For the past 12 years he has focused on integrating neuroscience findings into high fidelity security trainings and has been embedded in such trainings worldwide. Don teaches Responder Mental Health at the Harvard Humanitarian Response Intensive course. He maintains an active interest in research and is one of the authors of the Headington Institute Resilience Inventory.*

***Chris Williams** leads the CARE USA Security Unit. As a security professional, his experience spans a number of sectors and disciplines, and his recent work has focused on access and operations in high-risk or complex environments. Chris holds a BSc (Hons) in international disaster engineering and management from Coventry University and several postgraduate certificates in security and risk management.*

**Risk and Strategic Management Corp, 7180 Opal Road, Warrenton, VA 20186, USA*
E-mail: mike.blyth@rsmconsulting.us

***Humanitarian Psychological Services, 16 South Oakland Avenue #211, Pasadena, CA 91101, USA*
E-mail: donbosch@sbcglobal.net

†*CARE Security Unit, CARE, USA*
E-mail: 62willchris@gmail.com

Journal of Business Continuity & Emergency Planning
Vol. 14, No. 4, pp. 310–332

Andries Dreyer *is the Global Director (Training) for World Vision International's Office of Corporate Security. His background includes UN peace keeping operations, international war crimes tribunals and humanitarian relief. He studied for his MSc in risk crisis and disaster management at the University of Leicester and has contributed to several books on operational security management, risk management and training and development.*

Aidan Hales *is an experienced leader in organisational resiliency, business continuity, crisis management, enterprise risk management and protective services. He holds Chartered Status within the Security Institute and is a Certified Protection Professional through ASIS. He holds an MSc in security management from the University of Loughborough and is a graduate of executive business and leadership programmes at the Wharton School of the University of Pennsylvania, Kellogg School of Business at Northwestern University and Georgetown University.*

Simon Mallett *is Head of Risk Consulting and Operations for Risk and Strategic Management, Corporation. Simon is a former British army officer and certified ISO 22301 Lead Auditor who has led the development of business continuity management systems for companies of all sizes across various sectors. He has developed and implemented business continuity plans and procedures for the management of serious infectious disease outbreaks, and for the deterioration of security risk environments in various countries.*

ABSTRACT

Humanitarian aid and development is a multi-billion-dollar sector, representing millions of organisations, with hundreds of millions of employees and volunteers operating worldwide. The community is, by its very nature, drawn towards danger, supporting vulnerable parties in high-risk 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 is growing. At the same time, expectations regarding the sector's duty of care are mounting, and employees, families, donors and governments are holding organisations increasingly accountable for their actions. Where an organisation fails — or is perceived to have failed — the people it is supposed to protect, it can face catastrophic litigation and reputational harm. Hostile environment awareness training 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 organisation. This paper discusses what drives the increasing need for hostile environment awareness training (HEAT), the value it brings in terms of duty of care and organisational resilience, what technical content and immersive learning should be included within a HEAT curriculum, and the challenges organisations face when implementing instruction programme at the global and multicultural level.

Keywords: hostile environment awareness training, HEAT, security, risk, SSAFE, travel risk management, duty of care

Andries Dreyer

Aidan Hales

Simon Mallett

INTRODUCTION

In the last 20 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 organisations 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

[†][†]World Vision, 800 West Chestnut Ave., Monrovia, CA 91016, USA
E-mail: andries_dreyer@wvi.org

[‡]Kingwood, TX 77345, USA
E-mail: aidan.hales@gmail.com

[‡‡]Risk and Strategic Management, Corp., 7180 Opal Road, Warrenton, VA 20186, USA
E-mail: simon.mallett@rsmconsulting.us

organisations typically avoid or withdraw from such environments, humanitarian aid and development organisations actively head towards the danger or maintain missions, despite dramatic changes in the risk environment. Research by Smet *et al.*[1] indicates 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 professionalised resilience has grown, so that organisations can maintain or increase the tempo of operations under deteriorating risk conditions.

Organisational 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 that threaten the survival of those organisations delivering assistance. Where resilience is weak or absent, the negative implications for the organisation, 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 organisations from disruptive shocks to operational continuity, it is also necessary to meet the increasing demands of beneficiaries in uncertain and hostile environments.[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 organisational resilience in the humanitarian aid and development sector, focusing on the importance of using immersive learning (that is, learning that allows an individual, or group, to apply knowledge to a practical problem, and so learn by doing) 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, prioritise 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 ten senior security professionals, and a semi-structured interview pool of 32 sectoral risk professionals. To maintain confidentiality, interviewees have been pseudonymised unless the organisation they work for is specified, in which case their comments are fully attributed.

WHAT IS 'HEAT'?

The term 'HEAT' refers to hostile environment awareness training. The meaning of this 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 definition of what HEAT means, beyond that of preparing individuals to face an unusual

level of personal risk. Among security professionals, the debate focuses on six main areas:

- *Content*: What competencies are required? What associated knowledge and skills need to be taught, exercised and tested within a programme of instruction?
- *Delivery*: What methodology is used to deliver knowledge? This might include classroom-based teaching, tabletop exercises, discussion groups, practical sessions/exercising, e-learning or videogames.
- *Duration*: How much time is required to adequately teach, exercise and test the knowledge and skills being delivered?
- *Intensity*: How realistic and immersive does the learning experience need to be, and what resources are required to produce the required outcomes?
- *Testing*: Is the course a pass or fail experience? What are the testing criteria, and what are the implications for the individual and organisation if they fail?
- *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 there is ambiguity regarding 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 immersive experience in order to contextualise 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, resulting in significant variances in content and delivery. 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 in captivity), 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 organisations self-run training, there is more latitude to fail participants 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 the legal department to ensure there is no ambiguity regarding 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 organisation. Where organisations do require a pass or fail determination, then commercial trainers run the risk of being poorly graded by disgruntled participants.

Training methodologies can differ between organisations that self-run training, and those who provide it as a commercial offering. 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* as effective as 'boring' training

may result in weaker participant evaluations, thus dampening future business. As a result, commercial companies that need to motivate participation are more likely to dial up the 'Hollywood effect' compared with self-hosting organisations, which can mandate attendance. Commercial companies are heavily influenced by profit, with some investing heavily to generate a strong 'brand' and so provide more client engagement, while others streamline investments to maximise profitability where the brand factor is less important. Where commercial companies seek to create a brand, the training is more likely to be richly resourced, especially where investments are then leveraged across multiple clients, or are capitalised across multiple organisations and time. Where training is self-run, then investment is more typically applied to a single organisation (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. Commercial companies may provide experts from the field of post-traumatic stress disorder and counselling; however, the sending organisation(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, any immersive learning experience must give careful consideration to the mental wellbeing of attendees and must be maturely configured to ensure positive — not damaging — learning outcomes. In this regard, well-designed and sensitively constructed training is essential; as one respondent commented during the interviews for this study:

> '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.' (Global Director of Security for a non-governmental organisation)

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 organisations 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 that sits atop a number of levels. Scalability is required to give organisations 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-box exercise, focusing on economic savings rather than 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 evaluated effectively to enable organisations to measure learning experiences gained from other organisations or commercial providers, or where government or military training programmes — such as survival, evasion, resistance and escape (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 learned 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.

The findings from the interview pool suggest that some decision-makers seek content and course duration ambiguity within HEAT courses to reduce organisational accountability. If a standard is hard-coded into a course, then any failure to meet this standard will expose the organisation to legal and reputational risk. This presents a potential clash between the security professional seeking to protect the individual, and the organisation's legal department, seeking to safeguard the organisation from tort lawsuits. From a legal and reputational standpoint, those organisations that 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 the organisation can arguably claim 'arms-length distance' liability protection. As a result, HEAT means different things to different people. As one interviewee commented:

> 'The word HEAT shouldn't exist in my opinion at all … it is all over the place, and it needs to be standardised.' (Director of Training for a large non-governmental organisation)

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 Safe and Secure Approaches in Field Environments (SSAFE)[5] programme 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 stabilisation;
- Indirect and direct small arms fire attacks;
- Post-traumatic stress disorder (PTSD) awareness;
- Basic self-defence;
- Information security awareness;
- Communicating under duress;
- Effective team leadership;
- Cultural awareness;
- Criminal threats and responses;
- Hotel and guesthouse security;
- Risk awareness for lesbian, gay, bisexual, transsexual, queer, intersexual, asexual (LGBTQIA) groups;
- Gender security risks;
- Awareness regarding mines, improvised

explosive devices and unexploded ordnance;
- Anti-carjacking techniques;
- De-escalation techniques;
- Legal and illegal checkpoints;
- Emergency equipment and 'grab bags';
- Trip planning and risk avoidance; and
- Arrest and detentions.

Regardless of the duration or curriculum, a HEAT course seeks to build the resilience of the participants, enabling them to address personal and group risks effectively by reacting quickly 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' from which to select when faced with predicted threat situations. This is especially important as stress and fear can result in the release of cortisol, making people faster and stronger, while also compromising cognitive functioning — that is, 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 organisations to select from a sliding scale of HEAT variants that 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.

While the focus and weighting of course content, coupled with how theory, practical and immersive learning techniques are applied is currently ill-defined within the sector, there is a growing requirement to establish some degree of consistency for how HEAT curriculums are developed, and how courses are then run. Within such a hotly disputed field that seeks to address a complex interplay of factors, no single solution is likely. A more realistic goal is to establish sector-based principles for thematic areas of learning and defining where theory, practical and immersive learning techniques are most preferred. One technique is to identify the thematic areas of learning and then define — based on the risk environment to which participants will be exposed, where theory-based learning is sufficient, or where practical or immersive learning is needed to achieve the desired learning outcomes. Such an approach also makes it easier for security departments to present their case internally, and for organisations to justify the funding of training to donors. This matrix approach allows for variances in the focus of the content and the intensity of the experience, while providing a common framework that organisations can work to (see Table 1).

THE VALUE OF IMMERSIVE LEARNING

When faced with a unique and stressful situation, intuition tends to supersede analytical judgment, and people are more likely to revert to familiar actions than attempt a new and complex act that is more likely to save their lives. [6] Ripley's[7] 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 behaviour. This results in a sense of uncertainty that automatically engages the more primitive survival structures of the brain, reducing the ability to think clearly.[8] 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 recognise the effects that stress has upon them as an individual — having experienced it before — and will be more likely to prioritise effective

Table 1: Defining the learning techniques required for scalable HEAT programmes

	Low risk			*Medium risk*			*High risk*		
Learning point	*Theory*	*Practice*	*Immersive*	*Theory*	*Practice*	*Immersive*	*Theory*	*Practice*	*Immersive*
Risk evaluations	✓	✓		✓	✓		✓	✓	✓
International travel planning	✓			✓	✓		✓	✓	✓
Land-based travel risks	✓			✓	✓		✓	✓	✓
Personal security awareness	✓			✓	✓		✓	✓	✓
Cultural awareness	✓			✓			✓	✓	✓
Criminal risks	✓			✓	✓		✓	✓	✓
Female security awareness	✓			✓			✓	✓	✓
LGBTQIA security awareness	✓			✓			✓	✓	✓
Hotel and guesthouse security	✓			✓			✓	✓	✓
Casualty stabilisation	✓			✓	✓		✓	✓	✓
Information security	✓			✓			✓	✓	✓
Arrest and detention risks	✓			✓			✓	✓	✓
Active shooter threats	✓			✓	✓		✓	✓	✓
Social disorder — riots/hostile crowds	✓			✓	✓		✓	✓	✓
Kidnap and ransom	✓			✓	✓		✓	✓	✓
Indirect fire attacks	✓			✓			✓	✓	✓
Small arms fire threats	✓			✓			✓	✓	✓
Mines and booby traps	✓			✓	✓		✓	✓	✓
Unexploded ordnance	✓			✓	✓		✓	✓	✓
Improvised explosive devices	✓			✓	✓		✓	✓	✓
Letter/parcel bombs	✓			✓	✓		✓	✓	✓
Self defence	✓			✓	✓		✓	✓	
Negotiation strategies	✓			✓			✓	✓	✓
Anti-carjacking techniques	✓			✓	✓		✓	✓	✓
Legal and illegal checkpoints	✓			✓	✓		✓	✓	✓
Post-traumatic stress awareness	✓			✓			✓		
Pandemics and epidemics	✓			✓			✓		
Natural disasters	✓			✓			✓		
Effective communications	✓			✓	✓		✓	✓	✓
Small group leadership under duress	✓			✓			✓	✓	✓

Theory-based learning — the presentation of information for participant consumption; *practice-based learning* — including class-based discussion groups and table-top exercising; and *immersive learning* — the act of 'doing', resolving problems through interactive simulation scenarios

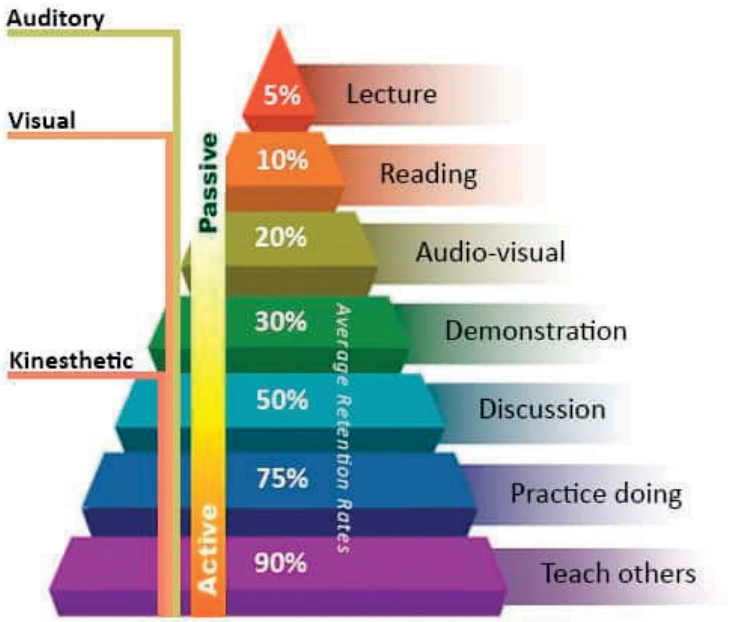


Figure 1: The applied behavioural science learning pyramid
Adapted from NTL Institute (1954)

courses of action to address real, rather than perceived, threats.

The vital importance of experiential or 'high-fidelity' learning is emphasised by Bosch, who comments that:

> '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 organisations best prepare employees deploying to high risk environments to not only avoid but also to survive a hostile security event should it occur.'[9]

These findings were supported by one of the interviewees, who commented that anyone travelling to a high-risk environment should be required to attend a HEAT course:

> 'I proposed to my President just yesterday, actually, that I wanted anyone travelling on assignment to go through a three-day HEAT training course, period. It should be required, end of story.' (Director of Security, global non-governmental organisation)

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 *behavioural*, which includes role plays, simulations and teach-backs.[10] The delivery of knowledge is then imparted through *visual*, *auditory* and *kinaesthetic* 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[11] 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. According to Chi *et al.*,[12] the following information retention rates are typical: reading — 10 per cent; seeing — 20 per cent; hearing — 30 per cent; seeing and hearing — 50 per cent; collaboration —70 per cent; and doing — 80 per cent. HEAT incorporates all forms of learning, and given that it teaches practical life-saving skills, requires an appropriate emphasis on 'doing' in order to be effective.

Immersive learning, through HEAT at

the individual level, or through emergency or crisis management exercises at the leadership level, provides an environment where learners develop and apply knowledge and skills on their own, or within a group of peers. It offers a framework where the individual must think actively 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. As Narli offers: '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'.[13] This is supported by Craik and Lockhart's[14] concept of the 'level of processing', which states that familiar and meaningful stimuli are better retained than less meaningful stimuli. Accordingly, HEAT must be realistic and relevant in order to resonate with the learner, and be viewed as meaningful and of practical value.

Knowledge retention and knowledge transfer are different.[15] 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 in 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, utilising 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 to overcome a stressful and fast-moving series of challenges. One interviewee commented on how HEAT builds individual resilience against safety and security challenges:

> '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 minimise the risk. They have the skills, knowledge and competency to solve problems, once they arise.' (Peter Sjøstedt, Global Safety Training Coordinator, Danish Refugee Council)

The curriculum of a HEAT programme should logically reflect the probable risks the individual may face, from low-probability and high-impact threats such as kidnapping, to high-probability and low to medium threats such as a mugging or natural disaster. As Kravitz and O'Molloy[16] posit: 'in many cases, simple training can go a long way to avoiding serious injury or death', and HEAT plays a key role in meeting the escalated risks employees face when working in areas subject to higher levels of crime, social instability, victimisation (notably for women and members of the LGBTQIA community), terrorism or war.

Feedback from HEAT participants is invariably positive, as individuals learn new knowledge and put this into practice within simulated scenarios. Feedback from

HEAT courses conducted by Risk and Strategic Management, Corp. underpins the need to blend theory with practical and immersive learning experiences:

> 'The course was extremely valuable — I will feel so much more confident in my travels as a result. A perfect blend of stress and distress. Such a cool facility to conduct training!'
>
> 'Very helpful and engaging teaching methods — my situational awareness has improved and I feel I have the skills needed for field work.'
>
> 'Excellent crisis preparation — I have the knowledge to reduce my risks. The high-stress simulations really helped to build critical muscle memory. The class-based learning is useful, but the real learning happened during the immersive parts of the course!'
>
> 'This type of learning needs to be put into action — it is all very useful to learn about high-risk situations, but to be put through your paces with professional role players and simulated gun-fire and explosions is where the learning really starts.'

HEAT not only offers value to the individual, but it also offers a mechanism for transformative change where organisations 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 organisation, rationalising 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 organisation, 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 the psychological wellbeing of people. However, duty of care is not just about protecting people; it is also about protecting the organisation from disruptive incidents — specifically from litigation and reputational harm. Duty of care includes two key elements: *action* and *evidence*. Not only is the organisation required to do the right thing, but it must also be able to prove it after the fact. The ability to evidence appropriate security steps to protect the individual enables organisations to demonstrate to employees, their families and to donors a professional approach to risk management. Guttry *et al.* note that:

> 'For international organisations, 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 organisations their legitimacy and credibility is put under risk, undermining the organisation's effectiveness.'[17]

Duty of care expectations have evolved over the past two decades and now demand that humanitarian aid and development organisations meet the same standards as their commercial counterparts, with Bickley[18] 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'. HEAT forms an important part of duty of care

requirements, with organisations increasingly being required to invest in immersive training. During the study, one interviewee commented:

> '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 physical hostile environment awareness training.' (Regional Security Director for a major humanitarian organisation)

Figure 2 represents the opinion of 77 seasoned security professionals when asked to respond to the statement: 'Organisations 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 per cent felt that organisations 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 and are invariably subject to low levels of risk; 2) international travellers who may operate in higher-risk and unfamiliar environments with limited to no supportive social networks and resources; and 3) host nation staff, who reside and work in their home country and who, while able to draw upon social networks, local experience and national resources, may be continually exposed to risk and are arguably are more vulnerable to targeting. This

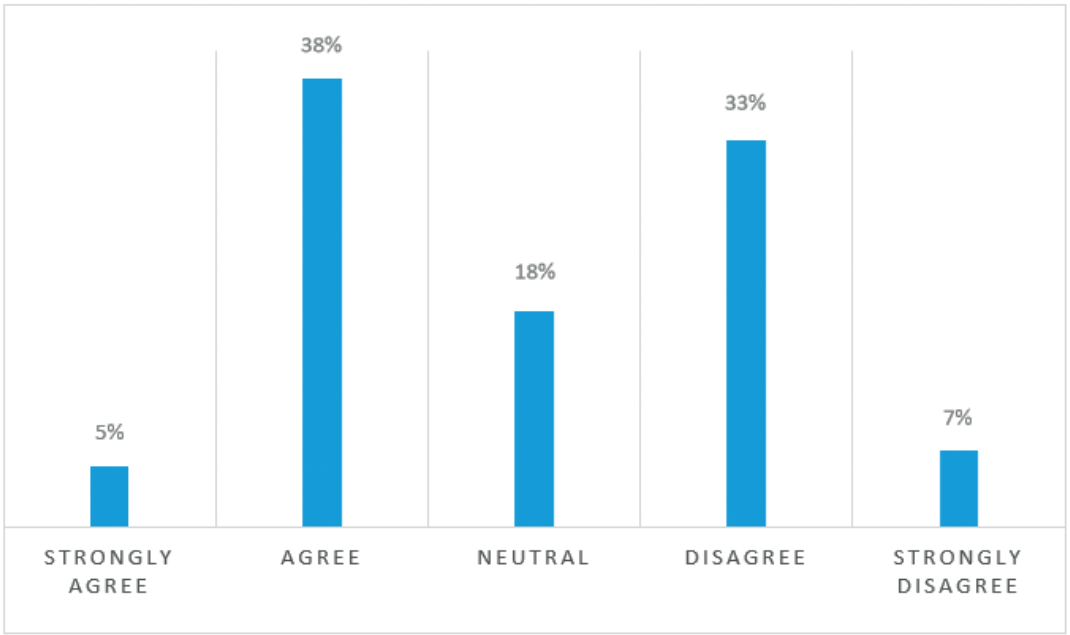


Figure 2: Response to the statement 'Organisations place great importance on building the knowledge, skill and confidence of the broader staff population in risk management at a personal level'

latter 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. One interviewee made the following comment in support of the view that individuals working together to resolve realistic problems within a HEAT course was beneficial in developing competency at the personal level:

> '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.' (Senior risk leader at the headquarters level)

Over the past decade, awareness regarding the importance of HEAT has grown, with international staff increasingly demanding immersive training before deploying to high-risk and unfamiliar environments. Host nation staff are likewise demanding some form of HEAT, as they recognise they face prolonged exposure to many of the same risks, despite working within their home country. Indeed, host nation staff form the largest portion of the learning population. As Jackson and Zyck[19] note, the value of training has seen a marked increase: 'in 2011 only 26 per cent of local NGO (non-governmental organisation) staff reported receiving security training, while that figure was 47 per cent in the latest (2015–2016) survey'. This resonates with the findings shown in Figure 2, which illustrates how 43 per cent of organisations surveyed now actively support individual-level security awareness training.

At this time, it is unclear whether the catalyst for change is organisations recognising and embracing the benefits of HEAT, or whether they have been forced to adopt this training to address external pressure. There is also debate regarding whether national staff warrant the same degree of training as those travelling 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 traveller.

As illustrated in Table 2, a large number of studies have explored the physical risks facing employees and volunteers within the sector, to clear up any ambiguity regarding the increasing probability that people will be exposed to, and be harmed from, security risks. According to Stoddard *et al.*,[20] 'INGOs (international non-governmental organisation) seem to be taking on greater risks than ever before', suggesting that the frequency and severity of security incidents, and subsequently risks, will only increase (with spikes occurring) over time.

The effects cascading from a security incident often exacerbate the disruptive impacts to the organisation and confuse risk control measures. Indeed, the secondary and tertiary risk implications of the incident are often more likely to cause strategic and lasting harm than the initial incident itself. These can also quickly deplete organisational capacity and resources, while overwhelming ill-defined and unpractised resistance measures.[21] Where risks are 'known,' they must be appropriately treated. According to Guttry *et al.*,[22] '[the] duty of care constitutes a non-waivable duty on the part of organisations to mitigate or otherwise address foreseeable risks that may harm or injure their personnel and their eligible family members'. The authors add that it is possible to prove when the duty of care has been violated by 'demonstrating the lack

Table 2: Summary of NGO security incidents, 2008–18

	2008	*2009*	*2010*	*2011*	*2012*	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*
Number of incidents	165	155	130	152	170	265	192	149	163	158	228
Total aid worker victims	278	295	250	311	277	475	332	289	295	313	408
Total killed	127	108	73	86	71	160	123	111	108	139	131
Total injured	91	94	84	127	115	179	88	109	99	102	146
Total kidnapped	60	93	93	98	91	136	121	69	88	72	131
International victims	51	74	41	29	49	60	32	29	43	28	29
National victims	227	221	209	282	228	415	300	260	252	285	379
UN staff	65	102	44	91	57	106	66	43	71	48	69
International NGO staff	158	128	149	135	97	142	152	173	159	98	183
Local NGO and Red Crescent Society staff	44	47	47	77	93	167	74	49	48	115	138
International Committee of the Red Cross staff	6	17	10	5	3	20	23	6	11	42	13

Source: Aid Worker Security Database (2020), available at: https://aidworkersecurity.org/

of measures adopted by the sending organisation to secure and guarantee the safety of personnel working on the ground'.

Legally, organisations are required to articulate risks, and to train people to address them. Lockton,[23] the world's largest privately held insurance brokerage firm, states that: 'organisations 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[24] define the requirement from both an ethical and legal standpoint, stating that 'safety and security are not only an ethical and moral concern but a legal obligation'. Furthermore, they extend this obligation beyond employees to include seconded staff, citing litigation from 2007 where the court ruled 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'. Where duty of care standards are not met, then both the individual and the employer suffer. During the interviews, a legal expert supported the need for a '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 organisations 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.' (Expert on Humanitarian Law)

Kemp and Merkelbach[25] reinforce the negative consequences of failing to meet appropriate duty of care requirements, stating that:

> 'The consequences of legal liability to international aid organisations 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'.

While the need for HEAT may not be universally agreed, its importance is nonetheless widely recognised.

Guttry *et al*.[26] 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 recognises the importance of providing its staff and their dependents with relevant security information, including both online and face-to-face security training, with up to a five-day HEAT programme for those working in high-threat environments. A similar model is used by the World Bank Group, the International Monetary Fund (IMF), the African Union and the Organisation for Security and Cooperation in Europe. 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[27] also recognises the risks individuals face, stating that: 'Delivering humanitarian assistance to vulnerable populations around the world often requires relief organisations to operate in insecure environments, putting non-governmental organisation (NGO) staff at risk of death, injury, or kidnapping', 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 increasing number of organisations that embrace HEAT, and so establish a sectoral standard against which all organisations 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 on memory retention and the 'forgetting curve', conducted by Ebbinghaus in the 1880s,[28] have been replicated by Murre and Dros.[29] These studies indicate that certain styles of learning have associated retention patterns, with retention studies ranging from three 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. Thus, 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 organisations should reinforce learning. While the optimal frequency for refresher training has yet to be formally defined, most organisations running HEAT or equivalent programmes agree that skill fade occurs between three to five years, with Table 3 showing the certification validity for major organisations running internal HEAT programmes. It is important to note that, while refresher training goals may be at the third or fifth year point, cost and logistical challenges (including international travel and

Table 3: HEAT refresher frequency

Organisation	*Certification validity*
Care International	5 years
United Nations	Open
World Bank Group	3 years
Danish Refugee Council	3 years
Norwegian Refugee Council	3 years
International Monetary Fund	3 years
World Vision	5 years

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 organisational 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 organisations like the World Bank and IMF refresh knowledge through e-learning and videogame solutions, rather than requiring participants to physically return to a training centre for the in-person learning experience.

THE PROBLEMS ASSOCIATED WITH HEAT

Research has identified three main challenges for organisations 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 organisation'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.

The ease of justifying the investment of time and money 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 argue the case effectively, qualitative and quantitative data are 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 organisation 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 prioritised against competing organisational demands. During the interviews, one well-established academic and renowned author on security risks in the humanitarian sector commented that while driver risk reduction data were 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 organisation'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.' (Security risk academic)

Most of those interviewed stated that they could readily cite anecdotal evidence

where such immersive learning had been useful, including dealing practically 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. One interviewee indicated that his organisation 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 per cent 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 per cent of graduates had experienced a critical incident following HEAT and that 98 per cent 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.' (Andries Dreyer, Director of Training for World Vision)

Where organisations 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, the professional is faced with a 'Schrodinger's Cat'[30] scenario where they are 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 HEAT is effective then participants will rarely, if ever, experience a serious security incident as the course is likely to have raised the situational awareness of the participant, and in so doing mitigated a wide range of risks. Building documented case studies is therefore impaired as the effectiveness of training reduces the number of available examples to illustrate the value of HEAT. Where unique incidents do occur, then the value of security knowledge and skill quickly becomes apparent. Edward Bunker illustrates the value of effective HEAT related knowledge during the 2016 Islamic Militant attack on the Splendid Hotel in Ouagadougou in Burkina Faso:

> 'I went downstairs to settle the bill around 20:30 and it was like a scene out of a movie with smoke, gunfire noise, explosions — but all outside of the walls. And a very, very empty and dark lobby … I ended up spending the night in my bathroom with my computer and — luckily — a good wi-fi connection. I was able to get in touch with family and friends and crucially also a security consultant from my organisation as well as

> the US embassy … staying in the bathroom was one piece of advice from the security consultant — to put as many doors between me and the militants. Another was to make as little sound as possible and turn the lights off … our security consultant was able to advise me that there were French forces in the building and the sounds they were making fitted with the likely pattern of events. They approached my door and I announced myself — as I had been advised. They told me to open the door slowly and there I saw three French troops with rifles pointing at me, along with some US soldiers.'[31]

Where quantitative data are 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, shows how risk control measures protect people, and reduces insurance costs, or business losses.

The ability to fund security training (if it is not funded by donors), can place a financial strain on organisations, especially those that have not included the cost of training into a programme budget from the outset. Where security funds are absent or limited, or where the funding mechanism prevents or hinders recovering training costs, then organisations are forced to fund training from available fee and overhead budgets. Historically, organisations 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, donors are increasingly recognising the value of such training, and are willing to fund it. Indeed, according to the ECHO report,[32] 'Most major donors are willing to fund security measures and training'. Nevertheless, despite donor willingness to support HEAT, many organisations 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[33] also notes that where organisations recognise 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 organisations actually implementing and sustaining security training'. 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[34] 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'.

Where organisations 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-building needs. One respondent 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.' (Global Security Director)

The challenge of identifying credible training providers and suitable venues for the immersive learning experience can devalue the perceived value of a HEAT programme 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. The Security Director stressed the need for well-designed training:

> 'I think really well-designed HEAT training is particularly useful.' (Global Security Director)

Other experts within the field of security supported the need for standardisation, with one emphasising the need to be able to benchmark against a consistent standard in order to measure the organisational effectiveness in managing increasingly complex risks:

> 'We need to have a standard. We need to have a benchmark to run to.' (Global Security Director)

The challenge then is to define what constitutes 'good' training, where organisations do not have an internal training team to conduct a HEAT course. Even where larger organisations 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 organisations holding third-party training centre status; 2) programmes of instruction that come with independently recognised credentials; 3) training institutions with a proven track record in both the technical area and, importantly, 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 organisations outsource HEAT, they must develop their own evaluation metrics, without the benefit of a standard to align to, in order to sift the wheat from the chaff. One interviewee commented that good providers do exist, and so resources are readily available to support HEAT programmes:

> '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.' (Global Security Director)

The production of knowledge strategy is currently ill defined, but nonetheless forms the cornerstone of what should be in a HEAT curriculum. Etienne Wenger[35] 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 within the sector present different belief systems that influence

how knowledge is 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 experts with a credible background, experience, credentials and competencies. Where possible, training design should be aligned to recognised third-party standards to enhance performance and demonstrate competency. These may include recognition as an approved training centre through the Institute of Leadership Management, through externally accredited quality assurance programmes, such as the City and Guilds Assured programme, or by aligning training against the forthcoming ISO 31030 standards for Risk Management — Managing Travel Risk.

Where the curriculum and instructor team are effective, then the next challenge is to find 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; for example, employees of the International NGO Security Organisation were arrested in Kenya for possessing wooden replica weapons in training.[36] The difficulty in finding an appropriate training venue, with supporting resources, was echoed during the interviews:

> '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.' (Peter Sjøstedt, Global Safety Training Coordinator: Danish Refugee Council)

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 neighbouring training compromises the flow and realism of the learning experience. Training in proximity to government forces can also conflict with the ethos of many organisations, requiring them to seek alternative venues.

Few, if any, humanitarian aid and development organisations, or even institutional development bodies, can self-fund and operate a suitable training venue that covers 50+ acres, is appropriately licensed, and which holds an armoury 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, organisations 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 organisations 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 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 protect people, but also their employers. 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 organisations (eg Care International, World Vision, the Danish Refugee Council, the Norwegian Refugee Council, World Bank and the UN) 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 proving the utility of the training.

The necessity of moving the agenda of effective training forward to a scalable standard must be both developed and recognised across the sector in order to meet the needs of both the micro and macro organisation. These standards will not only shape the curriculum and manner in which knowledge is imparted, practised and tested, but will also form the metric by which to evaluate internal training resources or commercial provider excellence. Concurrent with 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 organisations. These, then, can be presented internally to organisational decision-makers, as well as externally to donors, thereby demonstrating the importance of investing in high-fidelity training.

ACRONYMS:

Non-governmental organisation (NGO)
International non-governmental organisation (INGO)

AUTHORS' NOTE

The comments from the interviewees do not necessarily reflect the opinions of the authors.

References

(1) Smet, H. D., Schreurs, B. and Leysen, J. (2015) 'The Response Phase of the Disaster Management Life Cycle Revisited Within the Context of "Disasters Out of the Box"', Homeland Security and Emergency Management.
(2) Beal, H. L. (2015) 'Military foreign humanitarian assistance and disaster relief (FHA/FDR) evolution: Lessons learned for civilian emergency management response and recovery operations', *International Journal of Mass Emergencies and Disasters*, Vol. 33, No 2, pp. 274–309.
(3) United Nations Counter-Terrorism Executive Directorate (2020) 'The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism', United Nations Security Council publication.
(4) United States Agency for International

Development (2019) Section H, Request for Proposal subcontract award.
(5) United Nations Department of Safety and Security (2020) 'SSAFE course advert', available at: https://www.unssc.org/courses/safe-and-secure-approaches-field-environments-ssafe-surge-deployment-september/ (accessed 10th July, 2020).
(6) Kowalski, M. and Vaught, C. (2003) 'Judgment and decision-making under stress: An overview for emergency managers', *International Journal of Emergency Management*, Vol. 1, No. 3, pp. 278–289.
(7) Ripley, A (2008) *The Unthinkable: Who Survives When Disaster Strikes — and Why,* Three Rivers Press, New York.
(8) Brosschot, J. F., Verkuil, B. and Thayer, J. F. (2018) 'Generalized unsafety theory of stress: Unsafe environments and conditions, and the default stress response', available at: https://www.mdpi.com/1660-4601/15/3/464/htm (accessed 5th January, 2020).
(9) Bosch, D. (2015) 'Our Partnership with HEAT Trainings', Headington Institute, Pasadena, CA.
(10) National Highway Institute (NHI) (2020) 'Principles of Adult Learning & Instructional System Design', NHI Instructor Development Course Guide, available at: https://www.nhi.fhwa.dot.gov/downloads/freebies/172/PR%20Pre-course%20Reading%20Assignment.pdf (accessed 25th July 2020).
(11) Narli, S. (2010) 'Is a constructivist learning environment really effective on learning and long-term knowledge retention in mathematics? Example of the infinity concept', *Educational Research and Reviews*, Vol. 6, No. 1, pp. 36–49.
(12) Chi, M. T., Bassock, M., Lewis, M. W., Reimann, P. and Glaser, R. (1989) *Self-Explanations: How Students Study and Use Examples in Learning to Solve Problems*, Wiley and Sons, New York.
(13) Narli, ref. 11 above.
(14) Craik, F .M. I. and Lockhart, R. S. (1972) 'Levels of processing: A framework for memory research', *Journal of Verbal Learning and Verbal Behaviour*, Vol. 11, No. 6, pp. 671–684.
(15) Semb, G. B., Ellis, J. A. (1994) 'Knowledge taught in school: What is remembered?', *Review of Educational Research*, Vol. 62, No. 2, pp. 253–286.
(16) Kravitz, D. and O'Molloy, C. (2014) 'A risky business: Aid workers in danger', available at: https://www.devex.com/news/a-risky-business-aid-workers-in-danger-84373 (accessed 15th October, 2018).
(17) Guttry, A., Frulli, M., Greppi, E. and Macchi, C. (2018) *Duty of Care of the EU and Its Member States towards Their Personnel Deployed in International Missions,* Springer Books, Florence.
(18) Bickley, S. (2017) 'Security Risk Management: A Basic Guide for Smaller NGOs', European Interagency Security Forum, London.
(19) Jackson, A. and Zyck, S. A. (2016) 'Presence & Proximity: To Stay and Deliver, Five Years On', report commissioned by the United Nations Office for the Coordination of Humanitarian Affairs, available at: https://www.humanitarianoutcomes.org/sites/default/files/publications/presence_and_proximity.pdf (accessed 21st December, 2019).
(20) Stoddard, A., Harmer, A. and Czwarno, M. (2017) 'Behind the attacks: A look at the perpetrators of violence against aid workers', available at: https://www.humanitarianoutcomes.org/publications/aid-worker-security-report-2017-behind-attacks-look-perpetrators-violence-against-aid (accessed 10th July, 2019).
(21) *Ibid*.
(22) Guttry *et al.*, ref. 17 above.
(23) Lockton (2015) 'Duty of care: protecting traveling employees', available at: https://www.lockton.com/whitepapers/Duty_of_Care.pdf (accessed 10th December, 2019).
(24) Kemp, E. and Merkelbach, M. (2011) 'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff', Security Management Initiative,

available at: https://gisf.ngo/wp-content/uploads/2014/09/0197-Kemp-Merkelbach-2011-Can-you-get-sued%EF%80%A5.pdf (accessed 12th February, 2019).
(25) *Ibid*.
(26) Guttry *et al*. ref. 17 above.
(27) United States Agency for International Development (2018) 'Safety and Security Sector Update', available at: https://www.usaid.gov/sites/default/files/documents/1866/USAID-OFDA_Safety_and_Security_Sector_Update_-_FY_2018.pdf (accessed 15th June, 2019).
(28) Ebbinghaus, H. (1885) *Memory. A Contribution to Experimental Psychology*, Teachers College, Columbia University, New York.
(29) Murre, M. J. and Dros, J. (2014) 'Replication and Analysis of Ebbinghaus Forgetting Curve', US National Library of Medicine National Institutes of Health, Government Printer, Washington, DC.
(30) Yang, T. and Che, H. (2017) 'Quantum mechanics and multi-world interpretation — a dialogue between a cat and Everett', *Open Journal of Social Sciences*, Vol. 5, No. 1, available at: https://www.scirp.org/journal/PaperInformation.aspx?PaperID=73303 (accessed 20th November, 2020).
(31) BBC (2016) 'Burkina Faso hotel siege: "Like a scene out of a movie"', available at: https://www.bbc.com/news/world-africa-35333617 (accessed 26th November, 2020).
(32) European Civil Protection and Humanitarian Operations (2006) 'NGO Security Collaboration Guide', European Commission: Humanitarian Aid, available at: http://www.humanitarianaccess.eu/toolbox/Libreria/Manuales/EN/ECHO_NGO%20Security%20Collaboration%20Guide.pdf (accessed 28th November, 2020).
(33) Bickley, ref. 18 above.
(34) Brabant, K. V. (2010) 'Good Practice Review: Operational security management in violent environments', available at: https://doms.csu.edu.au/csu/file/1dcf1dcc-57a5-84bb-d330-473975a0affb/1/resources/readings/topic6_c_vanBrabant.pdf (accessed 13th October, 2020).
(35) Etienne, W. (1999) *Communities of Practice: Learning, Meaning and Identity*, Cambridge University Press, New York.
(36) ZeeNews (2020) 'Kenya arrests aid workers for wooden rifles training exercise', available at: https://zeenews.india.com/news/world/kenya-arrests-aid-workers-for-wooden-rifles-training-exercise_1612285.html (accessed 15th April, 2020).