Layered Security, Staff Training, Interoperability

Organisational Terrorism Mitigation

ANTHONY GLEDHILL

Layered Security & Protection in Depth

Staff Training

Interoperability

For

Organisational Terrorism Mitigation

Forward:

The primary objective of this resource and all the series e-books on protective security & counter terrorism is to support individuals and organisations in cultivating the right mindset and enhancing their abilities to design and implement organisational terrorism mitigation.

This approach is both economical and valuable, as it aids those who bear the responsibility for ensuring an organisation's resilience, safety, security, emergency response, crisis management, and business continuity.

It is important to note that the content of this e-book, along with all the series, should not be considered as absolute facts pertaining to risk management within the UK. Instead, they ar the opinions of the authors, shaped by their own encounters with private and public sector counter-terrorism operations.

Moreover, these resources offer an exceptional opportunity for security professionals seeking to improve their skill set specifically in the private sector's counter-terrorism domain. By accessing these e-books, they gain valuable insights and knowledge to enhance their expertise and contribute effectively to their organisation's security measures.

Table of Contents

Introduction

In this e-book, we delve into the implementation of Security In-Depth principles through a layered approach, staff training, and interoperability, demonstrating their adaptation to establish a robust organisational counter-terrorism protective security system. The methodology outlined here encompasses the vital aspects of deterrence, detection, delay, response, and recovery in the event of a terrorist attack (Purpura, 2008).

These security practices fall under the umbrella of physical protection systems (PPA), a time-tested and internationally recognised approach for both protective security and counter-terrorism spanning several decades. Typically involving a combination of people, procedures, and equipment, a PPS demands a systematic approach for its efficacy.

This e-book guides you through the intricacies of creating a comprehensive system, taking into account available resources to ensure the provision of necessary levels of protection, particularly in critical zones such as target-rich areas (Garcia, 2008).

International Management Standards

Organisations use their own hybrid management standards or adopt recognised systems such as ISO, British Standards or ASIS systems. The following information uses examples from all types of references, the point to keep in mind is that no matter what management systems are used by an organisation the following can be adapted to fit into any management standards.

Layered Security Systems

Layering Counter Terrorism Protection

During the design of a CT programme, protection must be delivered using multiple security approaches known as layering for protection (Fennelly 2013). The basic principles of protection in-depth have been added to by Patterson (2013), where he asserts using complementary controls moving from the outer perimeter to the centre to deter/displace; distinguish; delay; detect; trigger and deny adversaries.

This gives the CT programme designer multiple principles that can be adapted for counter-terrorism programme planning to integrate people, procedures, and equipment to protect the organisation and its operations.

System Framework

The protective security system will involve information security, personnel security; physical barriers; access controls; intrusion detection; CCTV; staff training; emergency response; and contingencies for protection in-depth using crisis management, business continuity plans and insurance mitigation (ANSI/ASIS PAP 2012).

Specific Risk Analysis & Plan (Note: Comprehensively explained in its other e-books within the series)

The risk analysis (RA) must be tailored to meet the specific objectives to mitigate the terrorism threat. The RA will characterise the organisation & needs; define the threats and identify the vulnerabilities; understand the adversary's capabilities and tactics; estimate the criticality of each event and produce a threat event profile that includes costs and time (Garcia 2008).

The design and plan must also be compatible and consider the organisation's resources and economic constraints (ASIS FPSM 2009).

To put the latter into context, a large organisation with thousands of staff & footfall, with multiple departments covering all the management systems to enable the business to function efficiently, will require a comprehensive CT risk analysis, design and implementation plan. A small business with just over a 100-footfall capacity and approximately 10 to 15 staff will probably require a less complex CT plan with emergency response training and one document that captures all the CT requirements.

21st Century Threats

When defining the treat, planners should consider the new terrorist threat objectives and research their capabilities and characteristics of aiming to inflict an escalatory pattern of violence, innovation in using weapons and tactics, and a willingness to take risks with their own lives to achieve their aims (ASIS POA Terrorism 2006). The Mildot article on 21st Century Terrorism explains the new characteristics of terrorist objectives.

The e-book on CT Needs & Risk Assessment follows the above process and explains multiple threats and vulnerabilities that apply to organisations. The below information can be used within the Risk Analysis recommendations to senior management to display how proven long-standing security principles are adapted and deployed for protective security systems to mitigate Terrorist Threats.

Creating a Secure Venue (as practicable)

The counter-terrorism programme planning process can be split into three main elements; detection, delay, and response (Patterson 2013). The following security measures will give examples that can be adapted for various facilities, from target-rich environments like retail and night-time economy facilities to open crowded venue spaces (Purpura 2008).

What measures can be applied to the protective security system will depend on the characterisation of the facility as explained in the risk analysis report, with areas identified as vulnerable receiving the greatest attention for mitigation options, such as target-rich choke points and entrances etc (FEMA-426 2011):

Detect. Detection also involves prevention, deterring and distinguishing. The mere presence of physical, technical, and information security measures can create an atmosphere of a security-controlled area, dissuading adversaries from committing the attack during their target identification stage (Purpura 2008). The more security measures for attackers to defeat and meet their aims add to the likelihood of preventing attacks on your specific location (ASIS PAP 2012).

One of the principles of crime prevention through environmental design is natural territorial reinforcement which can emphasise a security-controlled environment and deter/displace attacks (ASIS CPTED 2009).

External

External security measures include perimeters marked with security sings; clear lines of sight from the facility onto all perimeter areas allowing for natural surveillance from anybody on site (Fennelly 2013); Monitored CCTV coverage of the whole perimeter and access control points; frequent security patrols and all access points not operated require intrusion detection and CCTV; security personnel and staff must be trained in situational awareness, behavioural observation, emergency response and rapid reporting procedures (Riley et al, 2014).

Internal

Internal security measures to develop the organisation's culture and mitigate terrorist activity will require information and personnel security policies that control access to information and monitor with audits conducted; detail the organisation's open-source information guidelines and cyber security practices to prevent and deter terrorists from exploiting internal information and the organisation's on-line presence information (ISO 27001:2005).

The organisation's online presence must be sanitised of information terrorists can exploit. Removing imagery, staff information, and site plans are all critical areas that will hinder pre-attack research by terrorists (CPNI no date). HR employee screening procedures and periodic follow-up background checks, with social media monitoring to mitigate the threat and staff reporting procedures, are required (Sennewald et al. 2003).

All staff can be utilised as force multipliers to assist the organisation in preventing, detecting, and deterring terrorist threats (CPNI no date). The organisation's staff must be trained to recognise hostile recognisance and terrorist activity to create the force multiplier approach (Riley 2014).

All staff must understand their role and what is expected of them to behave in a manner that develops and improves the organisation's security culture, regular training and understanding of all CT policies will add to the counter terrorism mitigation success (CPNI no date).

Staff require identification cards to distinguish them from visitors and customers; all visitors should have visitor identification cards issued (when practical); a rapid risk communication system must be used for reporting suspicious activity and communicating with staff and customers (Fennelly 2013); limit access to one access point for staff and another for customers and monitor by CCTV and access control technology (Garcia 2008).

Delay. An attacker must travel through the perimeter areas to reach their intended target-rich environment. The principle of delaying is to prevent or contain the attack at the earliest point of entry (Patterson 2013).

Measures

Measures to contain an attack can be engineering controls at entry points such as doors, shutters, solid walls, fences, and other manufactured barriers and controlled through manual or technical systems. Shelter-in-place locations can be identified and target hardening measures applied to selected internal access and areas of the site (FEMA-426 2011).

Permanent and hidden hostile vehicle mitigation (HVM) systems can be used to separate vehicle and people areas. Parking areas can have their own perimeter fencing and pedestrian access control points, control access using one entry point with double door systems separated by approximately 5 to 10 meters with internal shutters (ASIS FPSM 2009).

The CT programme training plan must effectively train all staff in emergency response actions, and develop their situational awareness and behavioural observation skills, as an effective response will assist the organisation's response and recovery process

Training

The staff training plan must be applied in a manner that continually develops positive habits and knowledge. Any organisation that thinks a once-a-year 2-hour session on CT is the way forward underestimates the requirements and does not understand how people learn and develop new skills. Habitual training in short bursts is the proven option and does not encroach into staff's normal working hours. This topic will be covered in its own article and published in due course.

Response & Recovery

These topics are critical to the success of protective security systems (Sennewald 2003). Response and recovery will be covered in detail in their own article and the following will give you an idea of what is required. The staff's primary response elements should be documented in the emergency response plans and cover what action is taken to deal with the shourt-term aspects of the event (attack).

This will involve rapid incident identification and risk communications between staff and customers. Some options are mass evacuation or shelter in place, emergency services informed, and facility lockdown or lockout (ASIS EM 2008).

The recovery elements in response to an attack are documented within the crisis and business continuity plans. The main aim of the crisis management plan is to maintain a viable recovery strategy and deliver an effective response to protect the staff, customers, and the organisation in a timely manner (ASIS BC 2011).

Business continuity plans prioritise key business processes and minimise business interruption by having plans and insurance mitigation to manage business recovery and business resumption (Walters et al., 2013).

Conclusion

The layered approach to securing a venue gives an organisation multiple options to create counter-terrorism protection in-depth systems. The type of facility will dictate what level of physical, technical, and procedural mitigation can be implemented (Crelinsten 2020).

The challenge for all organisations is designing a protective security system to mitigate terrorism, whether using hard or soft approaches, that will require customer and staff buy-in to meet the protective security aims. Without that support, the programme will not succeed (Schurman et al, 2020).

The public relations strategy of selling security within and outside of the organisation must be considered during the protective security planning stages to ensure support from customers and staff (Sennewald 2003).

Staff Training

Introduction

Many organisations persist in employing conventional approaches to staff training, which may prove inadequate in addressing the evolving challenges of the 21st century. To fortify organisational resilience against contemporary threats, there is a pressing need for a paradigm shift in staff training.

The current lag in adaptation to modern threats underscores the importance of embracing innovative strategies. Integrating progressive methods into training initiatives can substantially elevate business resilience, fostering a heightened state of preparedness in effectively countering terrorism and hybrid threats.

Dismissing the outdated notion that security concerns are solely the responsibility of security staff is no longer tenable in the dynamic threat landscape of the 21st century.

Defensive Measures

Most organisations rely on Defensive Measures as the foundation of their security systems. Defensive Approach (Reactive). This approach is characterised by responding to threats after they have already occurred, often when significant damage has been done and the costs are considerably high (ANSIASIS PAP, 2012). That's a 20th Century approach.

Considering the continuously evolving and complex landscape of contemporary threats, it is crucial to embrace a dynamic security strategy tailored for the 21st century. This strategy should not only rely on traditional defensive measures but also integrate both detection and prevention methodologies (Patterson, 2012).

By merging proactive detection techniques with preventive measures, organisations can more effectively foresee potential threats, address risks in real-time, and markedly strengthen their overall security stance (Purpura, 2008).

Force Multiplier Mitigation

How does an organisation create a Force Multiplier system with minimal costs and time?

To cultivate a security culture conductive to detecting and preventing adversaries with violent intentions, it's essential to implement better strategies. Businesses can adopt force multiplier detection and prevention approaches to significantly enhance their preparedness compared to organisations relying on outdated defensive systems that often find themselves reacting only after a violent incident has occurred and the damage is incurred.

By fostering a security culture, organisations can instil awareness and vigilance among employees. Regular training sessions can educate staff on recognising potential threats and suspicious behaviour, enabling early detection.

This approach not only minimises the risk of violent incidents but also positions the organisation to respond swiftly and effectively if any threat is identified. Ultimately, by prioritising a forward-thinking security culture and implementing force multiplier strategies, businesses can stay ahead in the constant challenge of safeguarding against adversaries with violent intentions and improve organisational resilience (Kayyem, 2022).

Left of Boom

The optimal and forward-thinking strategy for tackling contemporary violent crime involves concentrating on systems that mitigate the Left side of the violent act. This approach revolves around the early detection and prevention of adversaries with violent intentions before they can carry out harmful actions (Riley et al, 2014).

Implementing measures to detect and prevent on the Left side of the violent act signifies intervening at various time intervals – be it within seconds, minutes, hours, days, or even weeks. Organisations can effectively improve their ability to identify and address potential threats at different stages of the planning and execution process (Kayyem, 2022).

This multifaceted approach not only enhances the overall security posture but also provides a flexible and adaptive framework that can respond to varying levels of threat severity and lead times. By prioritising the Left side of the violent act, entities can proactively safeguard against potential harm and contribute to a safer and more secure environment (Riley et al, 2014).

Business Employees

The most valuable asset within any business is its staff. Although technical and physical security systems are integral components of an organisation's security infrastructure, their effectiveness is heavily dependent on the human element. Employees, being an essential part of the organisation, can play a central and pivotal role in detecting and preventing acts of violent crime.

By instilling a culture of awareness and vigilance among the workforce, organisations can harness the human element to act as a proactive line of defence. Employees can contribute significantly to the security posture by being attentive to their surroundings, recognising potential threats, and reporting suspicious activities.

Training programs that educate staff on identifying warning signs and responding appropriately further empower them to actively participate in the organisation's security efforts. While technology and physical measures provide a foundation for security, the human factor is indispensable.

Cultivating a security-conscious mindset among employees not only enhances the effectiveness of existing security systems but also creates a collaborative and resilient security environment within the organisation (Bradford, 2017).

Human Element

Employees are intimately familiar with their workplace, colleagues, and day-to-day operations. This level of familiarity empowers them to detect unusual or suspicious behaviour that might go unnoticed by security technology.

Since employees interact with each other regularly, they are often the first to notice changes in behaviour, signs of distress, or concerning remarks made by a co-worker, contractor, or visitor. Reporting such observations can be crucial in preventing potential violent incidents.

Humans possess instincts and intuition that can't be replicated by machines. A gut feeling or sense of unease experienced by an employee can prompt them to act or alert authorities, potentially averting a security threat (Riley, 2014).

In emergency situations, employees are typically on-site, enabling them to initiate immediate responses and implement safety systems effectively.

Companies can establish anonymous reporting mechanisms, allowing employees to share security concerns without fear of repercussions. This encourages open communication and information sharing, strengthening the overall security posture (Sennewald, 2003).

Educating employees on security systems particularly on Terrorism & Hybrid Threats, emergency procedures, and threat awareness equips them to respond appropriately and effectively to potential threats and actively participate in maintaining a safe environment.

Shopping centre example:

The effectiveness of individuals monitoring CCTV is contingent on their ability to discern relevant information. Many CCTV operators tend to engage in what is commonly referred to as "Looking and Hoping" when observing monitoring screens. However, a more proactive and efficient approach would be to adopt a "Looking and Hunting" mindset (Riley et al, 2014).

In this approach, operators actively scan the baseline, familiarising themselves with normal activities and patterns. Subsequently, they engage in a systematic search of identified anomalies, transforming their role into a force multiplier for security.

By actively hunting for irregularities or suspicious behaviour, CCTV operators contribute significantly to the early detection and prevention of potential security threats (Riley et al, 2014).

Training programmes that emphasise the importance of proactive monitoring, anomaly identification, and rapid response can empower CCTV operators to be more effective in their roles. This shift from passive observation to active surveillance not only maximises the utility of CCTV systems but also enhances the overall security posture by leveraging the human element as a force multiplier in the surveillance process.

A shopping centre may have around 10 security staff, most of whom are engaging in passive monitoring ("Looking and Hoping") due to insufficient knowledge and training. The reliance on infrequent training videos, potentially centred around terrorism awareness, could indeed lead to a checkbox approach rather than fostering a comprehensive understanding and preparedness.

To address this, it becomes crucial for shopping centres to invest in ongoing and practical training programmes for their security staff and all other staff (Force Multipliers). These programmes should not only cover the basics of behavioural observation but also focus on recognising a broader range of security threats, understanding the nuances of different types of criminal activities, and developing effective response strategies.

A critical topic to teach staff is a decision-making cycle, that involves Baselining + Anomaly = Decision (Riley et al, 2014). There is no point training staff safety and security subjects if they have no knowledge of how to make an effective decision using a basic mental process they can follow.

Encouraging a culture of continuous learning and engagement through regular drills, simulated exercises, and access to updated training materials can empower security personnel to actively contribute to the safety and security of the shopping centre. By elevating their skills beyond mere box-ticking exercises, security staff and all other staff can become a more formidable and responsive force in addressing potential threats and ensuring the well-being of the shopping centre's customers and assets.

Eyes & Ears

In a shopping centre with approximately 200 staff members, each person represents a valuable set of eyes and ears. When equipped with basic training in security awareness, these individuals collectively become a significant force multiplier in the effort to detect and prevent adversaries with violent intentions.

Harnessing the observational capabilities of the entire staff can significantly enhance the overall security posture of the shopping centre. By instilling a sense of shared responsibility and providing basic training on recognising suspicious behaviour, potential threats, and appropriate reporting procedures, the staff can serve as an active security force multiplier.

This approach not only broadens the coverage of surveillance but also fosters a collaborative and proactive security culture. When everyone is aware and empowered to contribute to the safety of the environment, the likelihood of detecting and addressing security threats early on increases substantially.

The combination of trained security personnel and an engaged staff, creates a more resilient and responsive defence against potential adversaries with violent intentions. While it's true that no security system or group of individuals can guarantee the prevention of all acts of violence, knowledgeable staff can indeed play a significant role in the detection and prevention of adversaries with violent intentions (Riley et al, 2014).

The goal is not to create an infallible defence but to establish a robust and layered security approach that maximises the chances of early detection and intervention. By recognising the limitations and acknowledging that every additional set of observant eyes contributes to the overall security posture, organisations can better leverage their human resources to enhance the safety and well-being of everyone.

Let's squash some myths!

The proposed UK counter-terrorism laws currently undergoing parliamentary consideration and will affect the private sector aim to mandate organisations to provide Counter Terrorism training for their staff. The primary goal of this training is to cultivate security awareness among employees, empowering them to identify individuals with violent intentions.

However, the effectiveness of such training is contingent on the continuous mental and subconscious alertness of individuals in their day-to-day activities. Merely having staff watch an online video once or twice a year, or attending a brief classroom session, risks reducing the training to a mere box-ticking exercise. This approach lacks efficacy as individuals may simply endure the training without genuine engagement. In reality, people often resist uncomfortable truths and may disengage during training sessions, mentally checking out for the remainder of the six-month interval until the next session.

This disengagement poses a significant challenge to fostering a security culture, as a substantial portion of employees may not actively contribute to the collective effort. Furthermore, may existing training programmes overlook the crucial element of decision-making processes.

Without a clear framework for decision-making, the knowledge imparted during training becomes impractical. It is imperative to integrate decision-making methods into the training, ensuring that staff can not only absorb the relevant information but also apply it in real-world scenarios and effectively communicate their observations.

Staff Training Methods

Outdated training approaches should be set aside in favour of modern systems, particularly in the context of security and Counter Terrorism training. The traditional method of educating staff solely for their specific roles is no longer adequate in addressing the evolving challenges in security.

In contrast to the narrow focus on individual job functions, a more holistic and comprehensive training approach is essential in the realm of security. This is especially true for Counter Terrorism training, where a broader understanding of potential threats and a collective sense of responsibility are crucial.

The shift in perspective requires acknowledging that security is a shared responsibility that extends beyond individual roles.

By embracing alternative training systems, organisations can better equip their staff with the multifaceted skills needed to navigate the complexities of security threats, including those associated with Counter Terrorism. This shift acknowledges the interconnected nature of security issues and emphasises the importance of a collaborative and informed approach to training.

One off training sessions are useless. The approach to use is what's called Toolbox Talks, these talks are short, targeted, and do not impact daily work activity. They must be frequent, and not last longer than 5 to 10 minutes.

The optimal time to conduct is just before staff start work, use it as the morning brief etc. The toolbox approach develops conscious and unconscious thinking and raises mental alertness for the majority.

Security Personnel (In-house & Contracted)

Public and private sector entities frequently enlist the services of private security companies to safeguard diverse locations, including public facilities, construction sites, shopping centres, attractions, and night-time economy venues.

The subsequent discussion will centre on contracted security, reiterating certain details provided earlier but within an alternative context. To validate the performance and efficacy of contracted security services. It's proposed that contract holders inquire about the following aspects when engaging with their security personnel and company directors selling security services.

Questions

Responses to these inquiries typically span from expressions of uncertainty to the provision of credible explanations, albeit with a higher incidence of uncertainty prevailing.

Purpose of On-site-Presence:

What is the purpose of your on-site presence?
This question seeks to ascertain the fundamental objectives guiding the security personnel's physical presence at the designated location.

Observation Criteria:

What are you looking for while observing the area?
This query aims to expose the specific factors or indicators that security personnel focus on during their surveillance of the designated area.

Behavioural Signals and Decision-making:

What human behaviour signals prompt you to scrutinise more closely and initiate your decision-making process?
This question delves into the triggers that prompt a closer examination of human behaviour and the subsequent decision-making process that ensues.

Decision-making Process:

What is your decision-making process when deciding how to act in any given situation related to your role?
Here, the focus is on understanding the structured approach security personnel undertake when making decisions in situations relevant to their responsibilities.

Decision-making Options:

What options does your decision-making process provide you with?
This question seeks to uncover the range of choices available to security personnel because of their decision-making process.

CCTV Operator Behaviour Analysis:

For CCTV operators – What are you looking for in human behaviour, and how do you describe that behaviour to colleagues after completing your decision-making process on how to respond?

Specifically directed at CCTV operators, this question explores the nuances of behaviour analysis through surveillance systems and the subsequent communication of observed behaviour to colleagues.

CCTV Operator Approach:

For CCTV operators – Are you just looking and hoping?
This question challenges the proactive approach of CCTV operators, questioning whether their actions are based on a purposeful observation strategy or if there is an element of uncertainty in their approach.

Reasons for Questions

These essential inquiries empower contract holders and management to gain precise insights into the services they are procuring and the value of security personnel at their sites. Succinct responses to the posed questions not only provide clarity but also articulates understanding of human behaviour and their role.

This, in turn, facilitates the adoption of credible and effective decision-making processes by the security personnel which in turn acts a force multiplier on prevention and detection of people with violent and criminal intentions.

Effectiveness & Purpose

In the absence of such foundational information, the operation of security without this information could be deemed ineffective and lacking a clear purpose for being there in the first place. Educating security staff to address the provided questions is a manageable and straightforward process as explained above. The knowledge is not rocket science, and security personnel can quickly develop the necessary understanding.

Security Foreknowledge

In the 21st century, security challenges have evolved, necessitating security staff to possess both actionable foreknowledge and robust decision-making systems. The dynamic nature of contemporary threats demands a proactive approach where security personnel are equipped with anticipatory knowledge to identify and respond to potential risks before they escalate.

Decision Making

Effective decision-making systems are crucial to navigating complex and rapidly changing environments. In essence, the modern security paradigm requires not only a responsive posture but also a proactive and predictive capability.

21st Century Staff Training

This shift acknowledges the importance of foresight and adaptive decision-making in safeguarding against a diverse range of threats characteristic of the 21st century. Without these security fundamentals your facility may as well use manikins as security staff.

Conclusion

It's imperative to discard out-dated training methods and embrace alternative systems. Recognising security as a collective responsibility demands a more holistic training paradigm that transcends individual job functions. Counter Terrorism training necessitates a broader understanding of potential threats and a cohesive, organisation-wide commitment to vigilance.

By adopting modern training systems, organisations can cultivate a workforce equipped with a diverse skill set, enabling them to navigate the intricacies of evolving security landscapes. This shift underscores the interconnected nature of security issues and emphasises the need for a collaborative and informed approach to training. Ultimately, embracing these progressive training methodologies is crucial for fostering a culture of awareness, adaptability, and collective responsibility in the face of contemporary security threats.

Staff training doesn't have to consume valuable working hours or divert employees from their regular tasks. Employing a focused and well-organised series of toolbox talks can yield considerably greater advantages, resulting in the establishment of an effective force multiplier system.

Using the above information, any organisation with contracted security services can promptly pose these questions to gain a clear understanding of the value they are receiving for their investment in contracted security.

Conversely, security providers can assess the quality of their services and invest in their staff and provide and higher level of trained personnel to acquire contracts.

Interoperability

Enhancing Private Sector Resilience with Emergency Services Knowledge

Introduction

In the dynamic landscape of security, emergency, and crisis response, understanding interoperability is a crucial factor for the private sector. This resource explores how comprehending interoperability can assist private sector organisations, shedding light on the joint systems used by the UK Emergency Services to respond to Terrorist and Hybrid threats.

Interoperability Unveiled

Interoperability, often an unfamiliar term within the UK private sector, holds the key to increasing resilience for private sector organisations. At the heart of emergency services' responses lies an overarching system known as JESIP, or Joint Emergency Services Interoperability Principles. This system promotes a common model for joint working during emergencies, emphasising the following key principles. (The following information is from the JESSIP website. https://www.jesip.org.uk/joint-doctrine/principles-for-joint-working/#).

1. **Shared Situational Awareness.** Encouraging the sharing of information among emergency services to develop a unified understanding of the incident's scale, scope, and risks.

2. **Co-Locate.** Advantages of physical or virtual co-location, enhancing communication and understanding among responders, particularly beneficial for incidents requiring a regional or national response.

3. **Communicate.** Emphasising meaningful and effective communication between responders and organisations from the initial call or contact.

4. **Coordinate.** Involving control rooms and responders at all levels to discuss available resources, activities, agree on priorities, and make joint decisions throughout the incident.

5. **Shared Understanding of Risk.** Promoting the sharing of risk assessments between services to prioritize actions and allocate resources effectively. The ultimate goal is a unified approach to incident management, enabling seamless integration of efforts from different services into a cohesive team.

Local Government Rold

Adding another layer to the JESIP approach is the involvement of Local Authorities. Despite having their own management systems, Las are expected to seamlessly switch to the JESIP approach during their support, adding complexity to joint operations.

Las will have their own management systems and lines of communication, this adds a layer of possible obstacles when it comes to rapid decision-making requirements.

Private Sector Integration

Understanding the interoperability principles of emergency services is paramount for the private sector. Without this understanding, organisations may inadvertently hinder effective responses, presenting obstacles to the goals of emergency services.

During the planning or review phases of security, emergency response, crisis management, and business continuity plans, insights into emergency services' requirements become vital.

Benefits of Private Sector Interoperability

Aligning with emergency services' expectations offers several advantages for the private sector:

1. **Improved Communication and Collaboration.** Fostered during crisis situations, leading to more effective joint responses to terrorist and hybrid threats.

2. **Timely Information sharing.** Facilitated through interoperability, allowing comprehensive understanding and better decision-making.

3. **Comprehensive Understanding of the Situation.** This reduces confusion and assists in both entities working from a common operating picture.

4. **Rapid and Efficient Response.** Enabled by a clear comprehension of the emergency services response system, crucial in containing and mitigating threats.

5. **Minimised Duplication of Effort.** Collaborating helps to avoid duplication of effort.

6. **Increased Adaptability.** Both entities can leverage each others expertise.

7. **Public Confidence.** When public and private sectors work together, it demonstrates a unified approach that will reassure all concerned on the effectiveness of a response.

8. **Comprehensive Security Plans.** Developed with JESIP principles in mind, contributing more effectively to shared goal.

9. **Optimised Resource Allocation.** Identifying potential gaps and overlaps in resources, ensuring well-coordinated and effective response efforts.

Key Questions for Consideration

During the planning or review of security and safety plans, organisations should consider asking the following questions:

1. **Alignment with Emergency Services Systems.** Do the plans align effectively with emergency services system?

2. **Integration of JESIP Principles.** Can we integrate any of the JESIP principles to enhance the organisation's resilience?

3. **Efficiency of Response Preparations.** Do the response preparations of the business hinder the efficiency of emergency services?

4. **Improving Communication.** How can we improve communication to ensure that the plans are compatible with emergency responders?

5. **Emergency Services' Expectations.** What are the emergency services' expectations regarding risk communications?

6. **Critical Information Availability.** Have we critical information available for emergency responders?

7. **Compatibility within a Centre.** Shopping Centre etc. Are the plans compatible with other units within the centre?

8. **Neighbouring organisation Systems.** Do the plans complement neighbouring organisation systems, do we need to instigate mutual agreements.

Conclusion

In conclusion, this information encourages organisations to recognise the importance of aligning resilience strategies with the services at the forefront of saving lives during potential Terrorist or Hybrid attacks.

By understanding and embracing interoperability principles, organisations not only prepare for specific threats but also enhance their overall crisis management capabilities.

Gaining a deeper understanding of the mindset and operational procedures of emergency services becomes a strategic advantage, positioning organisations to.

References:

ANSI/ASIS 2012. Physical asset Protection. Protection of Asset Manuals. ASIS International.

ASIS BC Guidelines 2011 – Business Continuity Guidelines. Protection of Asset Manuals. ASIS International

ASIS FPSM 2009. Facility Physical Security Measures Guideline. Protection of Asset Manuals. ASIS International.

ASIS Terrorism 2006. Terrorism. Protection of Assets Manuals. ASIS International

ASIS EM 2008. Emergency Management. Protection of Assets Manuals. ASIS International

ASIS CPTED 2009. Crime prevention Through Environmental Design. Protection of Asset Manuals. ASIS International

Richard Bradford 2017. Personal Security. Preparing for the unexpected in the Era of Crime and Terrorism. Amazon.

CPNI. Personnel & People Security. Available at: https://www.cpni.gov.uk/personnel-and-people-security

CPNI. Optimising People in Security. Available at: https://www.cpni.gov.uk/optimising-people-security

Ronald Crelinsten 2020. Routledge Handbook of Terrorism & Counter-Terrorism. Deanta Global Publishing Services.

FEMA-426 2011. Buildings and Infrastructure Protection Series. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings FEMA-426/BIPS-06. Edition 2. Available at https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf

Lawrence J Fennelly 2004. Handbook of Loss Prevention and Crime Prevention. Fourth Edition. Butterworth-Heinemann

Juliette Kayyem 2022. The Devil Never Sleeps. Hachette Book Group.

Lawrence J Fennelly 2013. Effective Physical Security. Fourth edition. Butterworth-Heinemann

Mary Lynn Garcia 2008. The Design and Evaluation of Physical Protection Systems. Second Edition. Butterworth-Heinemann.

ISO/IEC 27001:2005. Information Technology – security Techniques – Information security Management systems – Requirements. Edition 2013-11.

Phillip P Purpura 2008. Security & Loss prevention. Fifth Edition. Butterworth-Heinemann.

David G Patterson 2013. Implementing Physical Protection Systems a Practical Guide. Second Edition. ASIS International.

Patric V Horne & Jason A Riley 2014. Left of Bang. Black Irish Entertainment LLC

Charles A Sennewald 2003. Effective Security Management. Fourth Edition. Butterworth-Heinemann.

Isabelle Duyvesteyn and Bart Schurman 2020. Routledge Handbook of Terrorism & Counter-Terrorism. Deanta Global Publishing Services.

Robert J Fischer, Edward P Halibozek, David C Walters 2013. Introduction to Security. Butterworth-Heinemann.

Charles A Sennewald 2003. Effective Security Management. Fourth Edition. Butterworth-Heinemann.