Counter Terrorism Guide for Business Owners & Senior Management
What you need to know

Forward:

The primary objective of this book and all the protective security & counter terrorism book series, is to support and inform business owners and management about what is involved with private sector counter terrorism mitigation and demystify the whole subject area.

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.

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 the series of e-books, they can gain valuable insights and knowledge to enhance their expertise and contribute effectively to an organisation's security measures.

Table of Contents

Introduction

This book aims to provide clear and comprehensive insights into the realm of protective security for counter-terrorism (CT) mitigation. Its primary objective is to assist business owners, senior management, and security professionals with the necessary knowledge to execute robust CT policy and procedures for their organisations.

Until recently, both the private and public sectors in mainland UK showed little interest in designing and implementing counter-terrorism (CT) mitigation using protective security systems. Government agencies had minimal involvement in private-sector CT mitigation.

However, internationally, private sector CT mitigation has been in place for decades, where security professionals have successfully designed and implemented CT measures to safeguard thousands of employees and customers in countries facing terrorism, insurgency, and organised crime utilising similar tactics.

This resource will not go into all the reasons and what 21st century terrorism has evolved into, other e-books as part of the protective security & counter terrorism series explore those topics.

By gaining a deeper understanding of what private sector counter terrorism is all about, you will be better prepared to tackle potential threats effectively. One key aspect that will be explained is the option of adopting a structured method to create and implement a Terrorism Awareness and Management programme.

This approach will be thoroughly explained to facilitate its practical application within an organisation.

Furthermore, we will delve into the importance of cultivating a security-conscious organisational culture. It will outline how a well-implemented counter-terrorism (CT) programme can significantly enhance the overall security and safety of the business.

This entails fostering a sense of awareness and preparedness among all employees (Kayyem, 2022).

Notably, the methods employed in designing and implementing a CT programme may vary based on the organisation's size and available resources (Patterson,2013).

Regardless of the scale, the article will emphasise that effective implementation demands a detailed and structured approach involving all stakeholders.

Moreover, it will highlight the significance of ensuring total commitment from everyone involved, while also striving to ensure that employees comprehend the reasons behind the protective security system and how it serves to mitigate terrorism activities, ultimately safeguarding everyone involved.

Organisation Size

The following information in this e-book can be tailored to any size of business. The systems and processes will be similar, but the scale of the assessments and CT mitigation requirements will be significantly different for a micro business towards a large organisation.

Draft Bill on proposed UK Counter Terrorism Laws

The draft bill is called – Terrorism (Protection of Premises) Act 2023. It will be referred to as Martyn's law.

Owners and business leaders must acquire legal advice once or if the Bill is passed and becomes law probably in late 2024. The Bill includes large amounts of information revolving around responsibilities and what constitutes a premises that falls under the law.

You can seek advice from experienced in-house security professionals or specialist protective security advisors, they will walk you through the process of protective security requirements, with the added benefits of bridging the knowledge gap for all concerned within the organisation.

The key point to take away from the above, do not take legal advice from security advisors, take advice from legal professionals on the Bill, and take your lead from security advisors with regards to what protective security requirements require implementing for CT mitigation.

Understanding CT Requirements

Business owners and senior management stand to gain valuable insights by participating in a briefing or presentation on Private Sector counter-terrorism before commencing any planning.

There are two credible options available for this purpose: utilising the expertise of the in-house head of resilience and security or engaging the services of a consultant (Tucker et al. 2012). Regardless of the choice, the following key points should be covered in these presentations.

1. Overview of the 21st Century Terrorism Threats. The presentation should provide a comprehensive overview of the contemporary terrorism threats that businesses may face (Green et al. 2008).
2. Why the UK Government is Implementing New CT Laws. It is essential to explain the rationale behind the UK government's decision to implement new counter-terrorism laws.

3. UK counter Terrorism Laws. An explanation of the existing UK counter-terrorism laws and their implications for private sector organisations. Understanding these laws will help businesses comply with legal requirements while also ensuring effective CT mitigation strategies.
4. The current Situation for Private Sector CT Mitigation. The presentation should assess the present state of private sector counter-terrorism mitigation efforts.
5. The Expected New Situation When CT Mitigation is Implemented. Outline how counter-terrorism mitigation will impact the private sector once if implemented due to new laws or as part of business resilience and duty of care responsibilities.
6. Example Costs, Implementation Timelines, Staff Training Requirements. Address the financial aspects associated with implementing the CT programme. Additionally, share realistic timelines for the implementation process and outline the staff training requirements to effectively execute the proposed strategies.
7. How the CT Programme Fits into Your Organisation's Current Management Structure. The presentation should emphasise how the CT programme fits into the organisation's current management structure.

By covering these essential points, the briefing or presentation will equip business owners and senior management with a comprehensive understanding of private sector counter-terrorism and enable them to make informed decisions while planning and implementing effective CT policies and procedures.

Senior Management Buy-In

For an effective Counter Terrorism programme within any organisation, it is crucial to have buy-in and support from the owner and senior management (Sennewald, 2003).

The individuals responsible for planning, designing, implementing, and monitoring the programme should seek the endorsement and commitment of the organisation's leadership.

Having owners and senior management support is vital for several reasons:

1. **Resource Allocation.** Counter Terrorism programmes often require resources, both in terms of finances and personnel. When top-level management supports the initiative, it becomes easier to allocate the necessary resources and funding for its successful implementation (Sennewald, 2003).
2. **Organisational Culture.** When leaders demonstrate their commitment to the Counter Terrorism programme, it sends a strong message throughout the organisation about the importance of this initiative. It helps create a culture of vigilance and security awareness among all employees (Kayyem, 2022).
3. **Authority and Decision-Making.** Programme owners need the authority to make decisions and implement necessary changes promptly. Senior management buy-in ensures that these decision-makers have the support they need to act decisively and respond to potential threats effectively (ANSI/ASIS, 2012).
4. **Coordination and Collaboration.** Counter Terrorism efforts often involve multiple departments and stakeholders within the organisation. With management support, it becomes easier to foster collaboration and coordination among these different parties to ensure a cohesive and comprehensive approach.
5. **Endorsement from External Partners.** Externally, partnerships with emergency services, government entities, of other organisations are often critical for Counter Terrorism programmes. The support of senior management enhances the organisation's credibility and reputation, making it easier to form and maintain these partnerships.

6. **Long-Term Commitment.** Counter Terrorism is an ongoing effort that requires sustained dedication. The backing of owners and senior management reinforces the programme's long-term commitment, reducing the risk of it being abandoned or overlooked in the face of other priorities (ANSI/ASIS, 2012).

For a robust and effective Counter Terrorism programme, securing owner and senior management buy-in is a fundamental step. Their support provides the necessary foundation for successful programme development, implementation, and continuous improvement to safeguard the organisation against potential threats.

Designating the Design and Implementation Team

After obtaining the commitment of business owners and senior management, the next crucial step is to determine the most effective approach for designing and implementing a cost-efficient Counter Terrorism programme (ASIS EM, 2008). This process will vary based on the organisation's size and resources:

1. **Medium to Large Organisations:** In larger organisations with multiple departments, it's beneficial to establish a dedicated design team for the Counter Terrorism programme. The team should consist of key personnel who possess relevant expertise and experience in security, risk management, and crisis response. Alternatively, the organisation can leverage its existing crisis management team, if available, and equip them with additional training and resources specific to Counter Terrorism (ASIS BC, 2005).
2. **Small Businesses:** Small businesses may not have the luxury of forming a large design team due to limited resources. In such cases, they can assign the responsibility to a single individual, preferably someone with relevant knowledge or prior experience in security matters. This individual would lead the design and implementation efforts, but it's crucial that they receive strong support from the owner or senior management (Fennelly, 2004).

Additionally, even in small businesses, it is highly recommended to seek consultant assistance. Engaging external consultants in Counter Terrorism can fill any knowledge gaps and provide valuable insights and best practices. This consultancy expertise ensures that the programme is well-informed, comprehensive, and aligns with industry standards.

3. **Assessing In-House Expertise.** Regardless of the organisation's size, you should conduct a thorough assessment of the in-house skills and expertise. This evaluation will help identify strengths and weaknesses within the organisation's capabilities. If the necessary skills and knowledge exist within the organisation, it can lead to a more self-sufficient programme (ANSI/ASIS, 2012). However, if there are significant gaps, external consultancy expertise becomes even more critical.
4. **Balancing Costs and Effectiveness.** While using external consultants may incur additional costs, it is vital to view it as an investment in the organisation's security and safety. The expertise brought in by consultants can help design a more effective and tailored programme, potentially offsetting the initial expenses through better risk mitigation) Patterson, 2013).
5. **Collaboration and Decision-Making.** In either scenario, collaboration with relevant stakeholders is essential. The design team or individual leading the programme should work closely with different departments and personnel to ensure their perspectives are considered, and the programme addresses specific needs across the organisation.
6. **4-Phase Approach to CT Mitigation.** It's suggested the 4-phase CT mitigation system is used for the whole process. That systematic approach is covered in great details in another e-book which is part of the protective security & counter terrorism series.

The success of designing and implementing a cost-efficient Counter Terrorism programme relies on careful consideration of the organisation's size, available resources, and expertise.

Whether forming a design team or relying on an individual, seeking consultancy assistance, and fostering collaboration, the objective is to create a robust and proactive programme that enhances the organisation's security posture and preparedness against potential threats.

Consultants

Engaging the services of a consultant to guide the design team during the development of the Counter Terrorism programme can be highly beneficial for most businesses (Tucker et al. 2012). Here are the key advantages of using a consultant in this process:

1. **Expert Guidance.** Consultants specialising in Counter Terrorism bring extensive knowledge and experience to the table. They are well-versed in current best practices, industry standards, and evolving threats.
2. **Efficient Implementation.** Consultants can streamline the design and implementation process, saving time and resources.
3. **Enhanced Skills and Knowledge Transfer.** As the design team works closely with the consultant, they have the opportunity to up-skill themselves throughout the process.
4. **Customisation and Adaptation.** While consultants bring best practices, they also adapt those practices to suit the organisation's unique context. This customisation ensures that the Counter Terrorism programme aligns with the organisation's culture, operational procedures, and risk profile.
5. **Future Independence.** By working closely with a consultant, the design team gains the skills and knowledge necessary to maintain and monitor the Counter Terrorism programme independently. This capability allows the organisation to sustain the programme's effectiveness without relying on constant external support.
6. **Confidence and Credibility.** The involvement of a consultant lends credibility to the programme, both internally and externally. This can be crucial for gaining support from stakeholders and building confidence in the programme's ability to address potential threats.
7. **Long-Term cost Savings.** While there is an initial cost associated with hiring a consultant, the long-term benefits of having an in-house team with enhanced capabilities can lead to cost savings in the future. The organisation will be better equipped to respond to changing security landscapes without continuous reliance on external assistance.
8. **Compliance and Regulation.** Consultants often possess knowledge about regulatory requirements related to Counter Terrorism. Their guidance ensures that the programme aligns with relevant laws and regulations, avoiding potential legal issues down the line.

Utilising the services of a consultant to guide the design team in developing the Counter Terrorism programme brings numerous advantages.

From expert guidance and efficient implementation to up-skilling the team and ensuring future independence. Consultants can assist organisations to create a robust and tailored programme that enhances its security posture and readiness to tackle potential threats effectively.

Consultancy Advice

When seeking advice from security consultancies, in the realm of briefings on terrorism, there exist two distinct domains: Terrorism Studies and Anti & Counter terrorism mitigation (ASIS Terrorism, 2008).

From a strategic standpoint, investing time in receiving counsel on Terrorism Studies topics might prove inefficient if the primary goal is to understand the essential requirements for Counter Terrorism mitigation. The suggested focus, particularly for most of UK private sector organisations, should be on gaining insights into the practical implications of Counter Terrorism mitigation and understanding the actualities involved.

Redirecting attention towards real-world impact and the practicalities of Counter Terrorism mitigation is deemed a more judicious utilisation of valuable time for organisations receiving such briefings.

Arguably, the author suggests that certain consultancies may incorporate terrorism studies information to augment their advice and briefings, potentially compensating for a lack of hands-on experience in executing Counter Terrorism mitigation strategies.

The issue is particularly pronounced when dealing with advisors grounded solely in theoretical knowledge, highlighting a potential disparity between theoretical expertise and practical application in the realm of Counter Terrorism mitigation.

The above seven topics can be used to set the scope when seeking advice from security consultants to ensure advice covers the essential topics and not spread into information of no value.

Wasted Time & Effort

Suppose consultancy advice is not used at any point during the design and implementation and none of the team has up skilled their CT knowledge. In that case, the risks of the in-house team going off on tangents and creating unnecessary costs and delivering an ineffective system are higher.

Any management or security professional should be able to read and interpret the e-book series on protective security & counter terrorism to assist them in designing and implementing the programme with minimal consultancy support.

Needs Assessment & Risk Analysis (NARA)

Once the CT programme design and implementation method has been decided, no matter who leads the process, the starting point for any organisation is the Needs Assessment & Risk Analysis (NARA) (Tucker et al. 2012). The NARA involves a Needs, Threat, Vulnerability & Risk Assessment.

Other Books

The counter Terrorism NARA is covered in detail within another e-book that explains in what is required for a Needs, Threat, Vulnerability and Ris Assessment.

In short, the CT programme will revolve around Deter/Displace, Detect, Delay, Response, And Recover principles (Patterson, 2013). The NARA is the central document that guides each mitigation measure implemented for terrorism threats.

What's assessed within the NARA

The following is an overview of what's involved.

The needs assessment stage in designing a Counter Terrorism (CT) programme is a critical step that requires gathering comprehensive information about the organisation and produces a characterisation of the business (Garcia, 2008).
This information is essential to characterise the facility or facilities and understand the potential risks and vulnerabilities.

The following elements are key components of the needs assessment:

1. **Financials**. Understanding the organisation's financial situation helps in allocating appropriate resources for the CT programme and determining the budget required.
2. **Staff Numbers**. Knowing the number of employees and their roles helps identify personnel who may require specialised training or have specific security responsibilities.
3. **Assets**. Identifying and assessing the organisation's assets (both physical and digital) helps in understanding potential targets for terrorist threats.
4. **Footfall**. Analysing foot traffic or visitor numbers provides insights into the potential impact of an attack on potential financial losses and injured personnel.
5. **Daily Operating Costs**. Knowing the operating costs is crucial for assessing the financial implications of implementing security measures.
6. **Daily Revenue Figures**. Understanding revenue figures helps evaluate the potential economic impact of an attack on business operations.
7. **Reviewing Crisis and Business continuity Plans**. Evaluating existing crisis and business continuity plans helps identify areas of improvement and integration with the CT programme.
8. **Information & Physical Security Plans**. Assessing existing security plans ensures the CT programme aligns with and enhances these measures.
9. **Business Insurance**. Reviewing insurance policies helps understand coverage and potential gaps related to terrorism-related incidents.
10. **Legal Requirements and Advice**. Understanding legal obligations and seeking legal advice ensures compliance with relevant laws and regulations.
11. **Researching Terrorist Attacks**. Studying past terrorist attacks and their modus operandi helps in identifying potential threats and vulnerabilities.
12. **Characterising Current Security & Resilience Capabilities**. Evaluating existing security measures and resilience capabilities helps determine areas that need strengthening.

After collecting and analysing all the necessary information, the design and implementation team can proceed to conduct a threat, vulnerability, and risk assessment. A point to note, during the needs assessment phase, it could be possible that an organisation has already systems in place that meet the requirements for CT mitigation.

The team will then produce a report for senior management, outlining the CT programme requirements. The report should communicate the assessments and utilise risk models to present the following (Garcia, 2008).

1. **Cost & Time**. Assessing the potential impact of different threats in terms of their consequences, the costs associated with implementing countermeasures, and the time required for implementation.
2. **Mitigation Measures**. Recommending specific measures to mitigate identified risks and vulnerabilities, including physical security improvements, training programs, and crisis management protocols.
3. **Criticality**. Prioritising risks based on their criticality to the organisation's operations and potential consequences. The criticality report must explain information that displays the threat, likelihood, impact in costs & life's current mitigation, new mitigation requirements.

The design team will present these recommendations to decision-makers for review and sign-off. If necessary, further information and edits can be sought to ensure that the CT programme aligns with the organisation's goals and effectively addresses potential threats.

It's recommended that the report uses threat and risk reporting models to deliver targeted and usable information that assists decision makers.

Security Principles

The Counter Terrorism mitigation should be designed to follow these key security principles (Patterson, 2013):

1. Deter
2. Detect
3. Delay
4. Respond
5. Recover

By integrating these security principles into its policies and procedures, the organisation can create a comprehensive and proactive Counter Terrorism programme that protects against potential threats and enhances overall security and resilience.

Implementation Plan

The implementation of the Counter Terrorism (CT) programme is a collaborative effort that involves both internal and external stakeholders. It requires seamless integration with other organisational policies and procedures to ensure a comprehensive and effective approach to security and resilience.

The following is an outline of how the CT programme can be integrated into an organisation's existing security framework (Tucker et al. 2012):

1. **Information & IT Security.**
   . Incorporate CT-specific information security measures to protect sensitive data related to the threat and vulnerability assessments.
   . Implement IT security controls to safeguard critical infrastructure and systems from cyber threats related to terrorism.
   . the online presence assessment will dictate what website and social media information is edited.
2. **Physical & Technical Security.**
   . Enhance physical security measures to deter and detect unauthorised access to facilities and high-risk areas.
   . Implement surveillance and access control technologies to monitor and manage potential threats proactively.
3. **Human Resources & Personnel Security.**
   . Conduct rigorous background checks and screening processes for employees to prevent insider threats and unauthorised access.
   . Implement awareness and training programmes for staff to educate them on recognising and reporting suspicious activities.
4. **Emergency Response & Crisis Management.**
   . Integrate CT-specific procedures into the organisation's emergency response plans to ensure a swift and coordinated response in case of a terrorist attack.

. Establish clear lines of communication and command during crisis situations to facilitate effective decision-making.
. Develop rapid risk communication systems.

5. **Business Continuity & Resilience.**
   . Develop continuity plans that address the specific challenges posed by a terrorist attack to ensure minimal disruption to essential services and operations.
   . Enhance the organisation's resilience by building redundancy and flexibility into critical processes.
   . Develop staff aftercare initiatives.
6. **Risk Management & Governance.**
   . Establish governance structures and nominate personnel responsible for overseeing the CT programme's effectiveness and compliance.
7. **Training.**
   . Provide comprehensive training to employees at all levels on CT awareness, response systems, and reporting procedures.
   . Conduct simulations and exercises to test the organisation's preparedness and identify areas for improvement.

Increased Organisational Safety & Security

A well-designed and implemented protective security Counter Terrorism (CT) programme offers numerous added benefits for an organisation (ANSI/ASIS 2012):

1. **Saving Lives and Reducing Injuries.** The primary goal of a Counter Terrorism is to prevent or minimise the impact of terrorist attacks. By implementing effective security measures, the program can significantly reduce the risk of casualties and injuries in the event of an attack.
2. **Asset Protection and Disruption Mitigation.** CT programmes focus on safeguarding critical assets, infrastructure, and operations. By doing so, they help mitigate disruptions caused by potential attacks, ensuring the organisation can continue to function even in challenging circumstances.
3. **Avoiding Legal Liabilities.** In the aftermath of a terrorist attack, organisations could face legal liabilities if it is proven that sufficient security measures were not in place to prevent or respond to the incident. A robust CT programme helps protect the organisation from potential legal actions that could be financially devastating.
4. **Media Coverage Control.** An organisation that experiences a terrorist attack may attract intense media attention. A well-prepared CT programme can help control media coverage, ensuring that accurate information is disseminated and minimising the risk of misinformation and panic.
5. **Reputational Damage Mitigation.** Terrorist attacks can have a severe impact on an organisation's reputation. A proactive CT programme demonstrates the organisation's commitment to security and safety, which can help mitigate reputational damage and maintain stakeholders' trust.
6. **Maintaining Customer confidence.** Customers can clients often prioritise security when choosing a business partner. A robust CT programme provides reassurance to customers, enhancing their confidence in the organisation's ability to protect their interests.

7. **Supporting Organisational Sustainability.** A successful CT programme enhances the organisation's overall resilience. By effectively managing security risks and potential threats, the programme contributes to the long-term sustainability and continuity of the business.
8. **Fostering a Secure Environment.** A CT programme not only protects the organisation but also creates a safer environment for employees, customers, and visitors. This sense of security fosters a positive and productive atmosphere within the organisation.
9. **Enhancing stakeholder Confidence.** Investors, shareholders, and other stakeholders often appreciate an organisation's commitment to security. A robust CT programme can bolster confidence among stakeholders, leading to greater support and investment.
10. **Compliance with Regulatory Requirements.** In certain industries or regions, there may be specific legal requirements or regulations related to security and CT. A well-implemented programme ensures compliance with such obligations.

A protective security Counter Terrorism programme offers a multitude of benefits beyond the direct prevention of terrorist attacks. From safeguarding lives and assets to controlling media coverage and maintaining customer confidence, the programme plays a crucial role in protecting the organisation's reputation, sustainability, and overall success.

Training and Staff Disapproval Issues

Training and education are crucial elements in embedding the Counter Terrorism (CT) programme into an organisation's operating culture and ensuring its success. Effectively communicating the importance of the programme and developing employee situational awareness are key to fostering a security-conscious environment. The following points highlight the significance of training and employee support in the CT program (Riley et al. 2014).

1. **Weekly and Monthly Training.** Regular and ongoing training sessions are essential to keep employees informed about the CT programme, potential threats, and proper response. Weekly and monthly sessions ensure that the information remains fresh in employees' minds and encourages a continuous focus on security. The goal is to create staff habitual behaviour on all security topic's, thus creating a culture within the organisation that increases resilience for personnel and the business.
2. **Educating Staff for Situational Awareness.** Training should focus on developing situational awareness among employees. They should be trained to recognise and report suspicious activities or behaviours that could indicate potential threats.
3. **Embedding into organisational Culture.** By integrating CT training into the organisation's culture, security becomes a shared responsibility among all employees, not just a select few. This approach creates a culture of vigilance and proactive risk management.
4. **Minimal Impact on working Hours.** Effective training systems should be designed in a way that does not significantly disrupt employees' regular working hours. Short, focused sessions or briefings can be conducted during team meetings, allowing for seamless integration with work routines. The training system known as Toolbox Talks is the optimal method. This approach does not impact staff normal work tasks or time.
5. **Overcoming Denial.** Addressing the uncomfortable topic of terrorism requires sensitivity and a well-thought-out training approach. Delivering the training with factual information, real-life

scenarios, and practical action plans can help overcome denial and instil a sense of responsibility among employees.

6. **Employee support.** Employees are more likely to engage and support the CT programme if they understand its significance and relevance to their safety and well-being. Providing them with clear information about the programme's objectives and benefits fosters support and cooperation.
7. **Practical Scenarios and Drills.** Conducting practical drills and simulations based on real-world scenarios helps employees internalise their training and practice response procedures. These exercises enhance preparedness and build confidence in handling potential threats.
8. **Leadership Involvement.** The support and involvement of organisational leaders are crucial in demonstrating the programme's importance and setting the tone for a security-conscious culture. Leaders should actively participate in training and emphasise its significance to the organisation's success.
9. **Regular Updates and Refresher Training.** As the security landscape evolves, regular updates and refresher training are essential to ensure that employees stay informed about new threats and changes to response approaches.

A well-designed training and education program is vital in creating employee support and embedding the CT programme into the organisation's culture.

By fostering situational awareness and providing practical tools and information, employees become proactive contributors to the organisation's security and preparedness against potential terrorist threats. Staff become what's termed as Force Multipliers.

Conclusion

For small businesses, one or two people with consultant assistance can design and implement the CT programme effectively. For large organisations, involving a team of staff from specific departments, especially those related to overall risk management, is the best approach.

The Crisis management Team, with its expertise in handling emergencies, can be the ready-made team to design and deliver the CT programme.

The CT programme's success relies on educating employees and gaining their support. The training programme should aim to make terrorism awareness the responsibility of every individual in the organisation.

Constantly improving staff's situational awareness is crucial in shaping the organisation's security culture and how employees respond during an attack.

By incorporating the above elements into the CT programme and ensuring that training fosters a culture of vigilance and preparedness among employees, organisations can enhance their overall security posture and resilience against potential terrorist threats. Empowering employees with the knowledge and skills to respond effectively during critical situations is crucial for protecting lives and maintaining a safe working environment.

References:

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

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

ASIS BC Guidelines 2005. Business Continuity Guidelines. Protection of Asset Manuals. ASIS International.

ASIS 2007. Consultants as a Protection Resource. Protection of Asset Manuals. ASIS International.

ASIS 2008. Terrorism. Protection of Assets Manuals. ASIS International.

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

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

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

Robert J Fischer. Edward Halibozek. Gion Green. 2008. Introduction to Security. Eighth edition. Butterworth-Heinemann

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

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

Patrick Van Horne. Jason A Riley 2014. Left of Bang. Black Irish Entertainment.

James F Broder. Eugene Tucker 2012. Risk analysis and the Security Survey. Fourth Edition. Butterworth-Heinemann.