Security Hardening Guide

Practical Strategies for Enhancing Protective Security at Public Venues

A Cambridge Sentinel Technical Guide
Published by Rittel Consulting Limited

Document Version: 1.0
Publication Date: December 2025
Document ID: CS-SH-GDE-001

Executive Summary

Security hardening refers to the systematic process of strengthening physical and procedural defenses to reduce vulnerability to terrorist attacks and other security threats. This guide provides practical, evidence-based strategies for organisations responsible for publicly accessible premises and events, with particular focus on compliance with Martyn's Law and alignment with United Kingdom protective security best practices.

The guide is structured around five core security domains: perimeter security, access control, surveillance and detection, security staffing, and emergency response. For each domain, we provide an overview of key principles, practical implementation guidance, and considerations for integration with existing safety and operational requirements. The strategies presented are scalable and adaptable, recognising that security solutions must be tailored to the specific risk profile, operational context, and resources of each organisation.

Effective security hardening is not solely about physical barriers and technology. It requires a holistic approach that combines physical measures, procedural controls, staff competency, and organisational culture. Organisations that adopt a layered

defense strategy—implementing multiple, complementary security measures—achieve the greatest resilience against diverse attack methodologies.

This guide is intended for security professionals, facilities managers, venue operators, and compliance officers responsible for implementing protective security measures. It should be read in conjunction with statutory guidance from the Home Office and Security Industry Authority, as well as sector-specific guidance from organisations such as ProtectUK, the National Protective Security Authority (NPSA), and the Centre for the Protection of National Infrastructure (CPNI).

---

1. Principles of Effective Security Hardening

1.1 Risk-Based Approach

Security hardening must be grounded in a systematic assessment of risks specific to the premises or event. A risk-based approach involves:

Threat Assessment: Understanding the nature and likelihood of terrorist attack methodologies relevant to the venue type and location. Common threat scenarios include:

- Vehicle-borne attacks (ramming, vehicle-borne improvised explosive devices)
- Armed attacks (firearms, bladed weapons)
- Improvised explosive devices (person-borne, placed devices, parcel bombs)
- Hostile reconnaissance and attack planning

Vulnerability Assessment: Identifying weaknesses in current security arrangements that could be exploited by attackers. Vulnerabilities may include:

- Uncontrolled access points
- Inadequate surveillance of critical areas
- Insufficient staff training and awareness
- Lack of coordination with emergency services

Consequence Assessment: Evaluating the potential impact of a successful attack, considering factors such as:

- Potential casualties and injuries
- Economic disruption and recovery costs
- Reputational damage and loss of stakeholder confidence
- Broader societal and psychological impacts

The combination of threat, vulnerability, and consequence assessments produces a risk profile that informs prioritisation of security measures.

1.2 Layered Defense (Defense in Depth)

No single security measure is foolproof. Effective security hardening employs multiple, complementary layers of defense, ensuring that if one layer is breached, others remain in place to detect, delay, or mitigate the attack. Layers typically include:

Deterrence: Visible security measures that discourage attackers from targeting the premises (e.g., CCTV cameras, security personnel, signage)

Detection: Systems and procedures that identify hostile activity before or during an attack (e.g., surveillance, staff vigilance, intrusion alarms)

Delay: Physical barriers that slow an attacker's progress, providing time for response (e.g., perimeter fencing, access control, lockable doors)

Response: Procedures and capabilities for responding to detected threats (e.g., evacuation, lockdown, coordination with police)

Recovery: Plans and resources for restoring operations and supporting affected individuals following an incident (e.g., business continuity, crisis communication, victim support)

1.3 Proportionality and Reasonably Practicable

Security measures must be proportionate to the assessed risk and "reasonably practicable" in the context of the organisation's resources and operational requirements [1]. This principle, central to Martyn's Law, requires balancing the risk reduction achieved against the cost, time, and effort required for implementation.

Proportionality considerations include:

- Avoiding security measures that create new safety risks (e.g., impeding emergency egress)
- Ensuring measures do not unduly disrupt legitimate operations or customer experience
- Recognising that smaller organisations have more limited resources than large enterprises
- Prioritising high-impact, cost-effective interventions over expensive, low-impact measures

1.4 Integration with Existing Frameworks

Security hardening should be integrated with existing fire safety, health and safety, safeguarding, and business continuity frameworks. Integration ensures:

- Coherent emergency procedures that address multiple scenarios
- Efficient use of resources (e.g., shared training, unified governance)
- Avoidance of conflicting requirements (e.g., lockdown vs. evacuation)
- Comprehensive risk management across all hazard types

---

2. Perimeter Security

2.1 Objectives

Perimeter security aims to:

- Define the boundary between public and controlled space
- Deter unauthorised access and hostile reconnaissance
- Detect and delay attackers attempting to breach the perimeter
- Provide early warning to security personnel and emergency services

2.2 Hostile Vehicle Mitigation (HVM)

Vehicle-borne attacks have been a prominent feature of recent terrorist incidents in the United Kingdom and internationally. Hostile vehicle mitigation measures reduce

the risk of vehicles being used as weapons to ram crowds or breach perimeters [2].

HVM Strategies:

Fixed Barriers

- Bollards: Steel or concrete posts installed at vehicle entry points and along pedestrian areas
- Street furniture: Benches, planters, and sculptures designed to withstand vehicle impact
- Walls and kerbs: Raised barriers that prevent vehicle access whilst maintaining pedestrian flow

Removable and Retractable Barriers

- Rising bollards: Hydraulic or pneumatic bollards that can be lowered to permit authorised vehicle access
- Gates and barriers: Controlled access points for service vehicles and deliveries
- Temporary barriers: Deployable systems for events or periods of heightened threat

Design Considerations

- Crash-tested to recognised standards (e.g., PAS 68, IWA 14-1) to ensure effectiveness
- Aesthetically integrated into the public realm to avoid fortress-like appearance
- Positioned to prevent vehicles from gaining speed before impact
- Coordinated with emergency vehicle access requirements

Case Study: Following the 2017 Westminster Bridge attack, Transport for London installed hostile vehicle mitigation barriers along key pedestrian areas on bridges and near landmarks. The measures combined aesthetically designed bollards and street furniture with clear signage and maintained accessibility for emergency services [3].

2.3 Fencing and Physical Barriers

Fencing and physical barriers define the perimeter and control access points. Effective perimeter fencing:

Height and Construction

- Sufficient height to deter climbing (typically 2-3 meters for high-security applications)
- Anti-climb features (e.g., smooth surfaces, outward-angled tops, anti-climb spikes)
- Robust construction to resist cutting, ramming, or lifting

Access Control Integration

- Limited number of entry/exit points to facilitate monitoring and control
- Gates equipped with locks, access control systems, or security staffing
- Clear signage indicating authorised access points

Visibility and Surveillance

- Transparent or semi-transparent fencing to maintain natural surveillance
- Integration with CCTV systems to monitor the perimeter
- Lighting to deter hostile reconnaissance and enhance surveillance effectiveness

2.4 Landscaping and Environmental Design

Strategic landscaping can enhance security whilst maintaining aesthetic appeal:

Natural Barriers

- Dense planting, hedges, and berms to define boundaries and deter access
- Water features (ponds, moats) as physical barriers
- Topography (slopes, ditches) to channel pedestrian and vehicle movement

Crime Prevention Through Environmental Design (CPTED)

- Maximising natural surveillance through clear sightlines and visibility
- Defining public and private spaces to discourage unauthorised access
- Maintaining well-lit, well-maintained environments to deter criminal activity
- Designing spaces to encourage legitimate use and natural guardianship

---

3. Access Control and Screening

3.1 Objectives

Access control and screening aim to:

- Prevent unauthorised individuals from entering controlled areas
- Detect prohibited items (weapons, explosives) before entry
- Create an auditable record of who is present on the premises
- Deter attackers through visible security presence

3.2 Entry Point Management

Effective access control begins with managing entry points:

Channelisation

- Funnelling pedestrians and vehicles through defined entry points
- Physical barriers (fencing, bollards, queuing systems) to guide movement
- Clear signage indicating entry procedures and prohibited items

Staffing and Supervision

- Security personnel stationed at entry points to observe and challenge
- Customer service staff trained to recognise suspicious behaviour
- Coordination between entry staff and security control rooms

Ticketing and Validation

- Ticket checks to verify legitimate access
- Electronic ticketing systems with barcode or RFID validation
- Integration with access control databases to prevent unauthorised entry

3.3 Bag Searches and Screening

Bag searches and screening detect prohibited items before entry:

Search Protocols

- Random or universal bag searches, depending on risk assessment and resources
- Clear communication of search policies to visitors (signage, announcements)
- Designated search areas with privacy considerations
- Procedures for handling discovered prohibited items (confiscation, police notification)

Screening Technology

- Walk-through metal detectors for detecting metallic weapons
- Hand-held metal detectors for targeted screening
- X-ray scanners for inspecting bags and packages
- Explosive trace detection (ETD) for high-risk scenarios

Considerations

- Balancing security effectiveness with customer experience and queue times
- Training staff to operate screening equipment and interpret results
- Ensuring accessibility for individuals with disabilities or medical devices
- Data protection compliance for any personal information collected

3.4 Access Control Systems

Electronic access control systems restrict entry to authorised individuals:

Technologies

- Key cards, fobs, or proximity badges
- Biometric systems (fingerprint, facial recognition)
- PIN codes or keypads
- Mobile credentials (smartphone-based access)

Applications

- Back-of-house areas (offices, storage, plant rooms)
- Restricted zones within public premises (VIP areas, control rooms)

- Time-based access (restricting entry outside operating hours)
- Integration with intruder alarms and surveillance systems

Best Practices

- Regular audits of access permissions to remove lapsed users
- Monitoring and logging of access events for security review
- Fail-safe or fail-secure configurations depending on fire safety requirements
- Backup power supplies to maintain operation during outages

---

4. Surveillance and Detection

4.1 Objectives

Surveillance and detection systems aim to:

- Monitor premises for suspicious activity and security incidents
- Provide real-time situational awareness to security personnel
- Deter hostile reconnaissance and attack preparation
- Capture evidence for investigation and prosecution

4.2 CCTV Systems

Closed-circuit television (CCTV) is a cornerstone of modern security surveillance [4].

System Design

- Coverage of critical areas: entry points, public spaces, perimeters, car parks
- Camera placement to minimise blind spots and optimise image quality
- Appropriate resolution and frame rates for identification purposes
- Integration with lighting systems to ensure visibility in low-light conditions

Camera Types

- Fixed cameras for continuous monitoring of specific areas

- Pan-tilt-zoom (PTZ) cameras for flexible, operator-controlled surveillance
- Dome cameras for discreet monitoring in public areas
- Thermal or infrared cameras for low-light or outdoor environments

Recording and Storage

- Digital video recorders (DVR) or network video recorders (NVR) for footage storage
- Retention periods compliant with data protection regulations (typically 30 days)
- Secure storage to prevent tampering or unauthorised access
- Backup systems to prevent data loss

Monitoring and Response

- Live monitoring by security personnel in control rooms
- Video analytics to detect unusual behaviour or intrusions (e.g., loitering, perimeter breaches)
- Integration with alarm systems to trigger alerts and recording
- Protocols for responding to detected incidents

Data Protection Compliance

- Compliance with UK GDPR and Data Protection Act 2018
- Clear signage informing individuals of CCTV surveillance
- Legitimate purposes for surveillance (crime prevention, public safety)
- Access controls to prevent unauthorised viewing of footage
- Data subject rights (access requests, deletion)

4.3 Intrusion Detection Systems

Intrusion detection systems (IDS) alert security personnel to unauthorised access:

Technologies

- Motion sensors (passive infrared, microwave, dual-technology)
- Door and window contacts to detect opening

- Glass break detectors for forced entry through windows
- Perimeter sensors (fence-mounted, buried cable, microwave barriers)

Integration

- Connection to central monitoring stations or security control rooms
- Integration with CCTV to provide visual verification of alarms
- Automated responses (e.g., locking doors, activating lighting, alerting police)

False Alarm Management

- Proper installation and calibration to minimise false alarms
- Environmental considerations (weather, wildlife, building vibrations)
- Staff training on alarm response procedures
- Regular maintenance and testing

4.4 Public Address and Communication Systems

Effective communication systems enable rapid dissemination of information during emergencies:

Public Address (PA) Systems

- Clear, audible announcements throughout the premises
- Zoned systems to target specific areas
- Pre-recorded messages for common scenarios (evacuation, lockdown)
- Integration with fire alarm systems

Two-Way Radios

- Communication between security staff, management, and emergency services
- Encrypted channels to prevent eavesdropping
- Backup power and redundancy to ensure reliability
- Regular testing and maintenance

Digital Communication

- Mobile apps for staff communication and emergency alerts

- SMS or push notifications for rapid dissemination
- Social media monitoring for threat intelligence and public communication
- Integration with organisational communication platforms

---

5. Security Staffing and Training

5.1 Objectives

Security staffing and training aim to:

- Provide a visible deterrent to hostile activity
- Detect and respond to security incidents in real-time
- Implement security procedures and operate security systems
- Coordinate with emergency services and support incident management

5.2 Security Personnel

Roles and Responsibilities

- Static guards at entry points and critical areas
- Mobile patrols for perimeter and internal surveillance
- Control room operators for CCTV and alarm monitoring
- Incident commanders for coordinating emergency response

Competency and Licensing

- Security Industry Authority (SIA) licensing for security personnel [5]
- Sector-specific training (e.g., door supervision, CCTV operation, close protection)
- Counter-terrorism awareness training (e.g., ACT Awareness, Project Griffin)
- First aid and emergency response training

Deployment Strategies

- Risk-based deployment, with increased staffing during high-threat periods or events

- Visible presence to deter hostile reconnaissance
- Coordination with local policing and counter-terrorism advisers
- Integration with venue operations staff for comprehensive coverage

5.3 Staff Training and Awareness

All staff, not just security personnel, play a critical role in protective security:

ACT Awareness Training

- Action Counters Terrorism (ACT) training provided by ProtectUK [6]
- Recognising suspicious behaviour and items
- Reporting procedures and communication channels
- Response to different attack scenarios (Run, Hide, Tell)

Role-Specific Training

- Evacuation coordinators and fire wardens
- First aiders and medical response teams
- Customer service staff trained to challenge and report
- Management and supervisors for incident command

Scenario-Based Exercises

- Tabletop exercises to test decision-making and procedures
- Full-scale drills simulating terrorist attacks
- Coordination with emergency services (police, fire, ambulance)
- Post-exercise debriefs to identify lessons learned

5.4 Liaison with Emergency Services

Effective coordination with police, fire, and ambulance services enhances response capabilities:

Counter-Terrorism Security Advisers (CTSAs)

- Free advice and support from local police CTSAs [7]

- Site visits and vulnerability assessments
- Guidance on protective security measures
- Information sharing on threat intelligence

Emergency Service Familiarisation

- Inviting emergency services to visit premises and understand layout
- Sharing floor plans, access points, and critical infrastructure locations
- Coordinating exercises and drills
- Establishing communication protocols for incidents

Multi-Agency Response Planning

- Participation in local resilience forums and partnerships
- Coordination with neighbouring premises for mutual support
- Integration with local authority emergency planning
- Business continuity and recovery planning

---

6. Emergency Response Procedures

6.1 Objectives

Emergency response procedures aim to:

- Protect individuals from immediate harm during an attack
- Coordinate evacuation or lockdown as appropriate
- Facilitate emergency service response and investigation
- Support recovery and return to normal operations

6.2 Evacuation Procedures

Evacuation is appropriate when the threat is localised and individuals can safely exit the premises:

Triggers for Evacuation

- Fire or explosion
- Suspicious package or bomb threat
- Chemical, biological, or radiological incident
- Structural damage or collapse risk

Evacuation Planning

- Clearly marked evacuation routes and emergency exits
- Assembly points at safe distances from the premises
- Procedures for accounting for individuals (roll calls, visitor logs)
- Accessibility considerations for individuals with disabilities

Communication

- Public address announcements with clear, calm instructions
- Visual alarms and signage for individuals with hearing impairments
- Staff coordination to guide and assist evacuees
- Liaison with emergency services to confirm safe evacuation

6.3 Lockdown Procedures

Lockdown is appropriate when the threat is dynamic and evacuation would expose individuals to greater risk:

Triggers for Lockdown

- Armed attacker (firearms, bladed weapons) on or near the premises
- Hostile crowd or civil disturbance
- Airborne contaminant requiring sheltering in place

Lockdown Planning

- Designated lockdown areas (rooms with lockable doors, minimal windows)
- Procedures for securing entry points and restricting movement
- Communication methods for instructing occupants to shelter in place

- Criteria for ending lockdown and transitioning to evacuation or normal operations

Run, Hide, Tell

- National counter-terrorism guidance for response to armed attacks [6]
- **Run:** Escape if safe to do so, leaving belongings behind
- **Hide:** Find a secure location, lock doors, barricade if possible, stay silent
- **Tell:** Call 999 when safe, provide information to police

6.4 Incident Command and Coordination

Effective incident management requires clear command structures and coordination:

Incident Command System

- Designated incident commander with authority to make decisions
- Deputies to ensure continuity if the commander is unavailable
- Defined roles for communication, evacuation, first aid, and liaison with emergency services

Communication Protocols

- Internal communication between incident command and staff
- External communication with emergency services, providing accurate information
- Public communication to manage media and stakeholder inquiries
- Post-incident communication to support recovery and learning

Documentation and Debrief

- Recording decisions and actions during the incident for review
- Post-incident debriefs to identify lessons learned
- Updating procedures and training based on insights
- Supporting investigations and regulatory inquiries

---

7. Continuous Improvement and Governance

7.1 Regular Review and Testing

Security hardening is not a one-time activity but an ongoing process:

Periodic Risk Assessments

- Annual or biennial reviews of threat, vulnerability, and consequence
- Updates to reflect changes in operations, threat landscape, or regulatory requirements
- Engagement with counter-terrorism policing for threat intelligence

Procedure and Measure Testing

- Regular drills and exercises to test evacuation, lockdown, and incident response
- Functional testing of security systems (CCTV, alarms, access control)
- Maintenance schedules for physical security infrastructure
- Staff competency assessments and refresher training

Audit and Assurance

- Internal audits of compliance with Martyn's Law and other regulations
- External audits by security consultants or regulators
- Benchmarking against industry best practice and peer organisations
- Reporting to leadership and governance bodies

7.2 Lessons Learned and Adaptation

Learning from incidents, exercises, and sector developments ensures continuous improvement:

Incident Analysis

- Post-incident reviews to understand what worked and what did not
- Sharing lessons learned within the organisation and with industry peers
- Updating procedures and training to address identified gaps

Sector Engagement

- Participation in industry forums and information-sharing networks
- Monitoring guidance from ProtectUK, NPSA, CPNI, and the SIA
- Engaging with trade associations and professional bodies
- Contributing to sector-wide resilience and preparedness

7.3 Governance and Accountability

Robust governance ensures that security hardening receives appropriate attention and resources:

Board and Executive Oversight

- Regular reporting on security posture and compliance status
- Allocation of budget and resources for security measures and training
- Accountability for the responsible person and security leadership

Integration with Risk Management

- Security risks included in corporate risk registers
- Alignment with enterprise risk management frameworks
- Coordination with health and safety, fire safety, and business continuity

Stakeholder Communication

- Transparency with staff, customers, and stakeholders about security measures
- Engagement with local communities and authorities
- Building confidence through visible commitment to safety and security

---

8. Conclusion

Security hardening is a multifaceted discipline that combines physical measures, procedural controls, staff competency, and organisational culture to reduce vulnerability to terrorist attacks and other security threats. Effective security hardening is risk-based, proportionate, and integrated with existing safety and

operational frameworks. It employs layered defenses, recognising that no single measure is foolproof, and prioritises continuous improvement through regular review, testing, and learning.

For organisations subject to Martyn's Law, security hardening is both a legal obligation and an opportunity to enhance resilience, protect people, and demonstrate corporate responsibility. The strategies outlined in this guide provide a practical foundation for implementing protective security measures tailored to the specific risk profile and operational context of each organisation.

Rittel Consulting Limited offers comprehensive support for security hardening, including risk assessments, design and implementation of physical and procedural measures, staff training, and ongoing compliance assurance. Our team of protective security specialists brings deep expertise in counter-terrorism, physical security, and regulatory compliance, ensuring that your organisation achieves both compliance and genuine security improvements.

References

[1] UK Parliament. (2025). *Terrorism (Protection of Premises) Act 2025*. Retrieved from https://www.legislation.gov.uk/ukpga/2025/10/contents

[2] National Protective Security Authority. (2025). *Hostile Vehicle Mitigation (HVM)*. Retrieved from https://www.npsa.gov.uk/specialised-guidance/hostile-vehicle-mitigation-hvm

[3] Transport for London. (2018). *Hostile Vehicle Mitigation on London's Bridges*. Retrieved from https://tfl.gov.uk/corporate/safety-and-security/security-on-the-transport-network

[4] US Department of Homeland Security. (2013). *CCTV Technology Handbook*. Retrieved from https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf

[5] Security Industry Authority. (2025). *Licensing and Standards*. Retrieved from https://www.gov.uk/guidance/learn-about-sia-licensing

[6] ProtectUK. (2025). *ACT Awareness Training*. Retrieved from https://www.protectuk.police.uk/training-and-exercises/act-awareness

[7] ProtectUK. (2025). *Counter Terrorism Security Advisers (CTSAs)*. Retrieved from https://www.protectuk.police.uk/advice-and-guidance/counter-terrorism-security-advisers-ctsas

---

Document Information

Author: Rittel Consulting Limited
Publication: The Cambridge Sentinel Technical Guide Series
Version: 1.0
Date: December 2025
Document ID: CS-SH-GDE-001

Disclaimer: This guide provides general guidance on security hardening and should not be considered a substitute for professional security advice. Organisations should consult with qualified security professionals to address their specific circumstances.

The Cambridge Sentinel is a service line of Rittel Consulting Limited, providing protective security intelligence and compliance guidance to organisations across the United Kingdom.