HMIC

Inspecting policing
in the public interest

An HMIC report on critical incident management by forces in England and Wales

Executive Summary

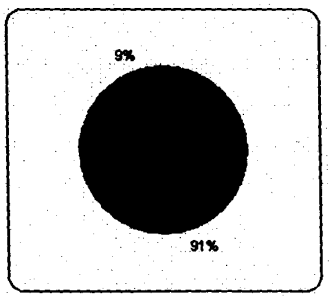
In handling many incidents of a critical nature, the service gets it right most of the time; but if just one case goes badly wrong and the police response has been demonstrably ineffective, it can leave a legacy that devastates a force's reputation for months and years to come.

Risk Management (RM) needs to be at the top of the management agenda, and RM techniques need to draw on leading edge thinking from across the public sector, internationally, and the private sector too. NPIA has an important role here but forces can do much for themselves by making the best use of the information and intelligence they currently collect and analyse (especially at the community level), to minimise and mitigate risk.

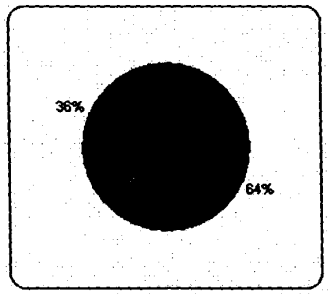
HMIC's review of Critical Incident Management is one of a series relating to Protective Services – those aspects of policing which require forces to lift their focus above local and predictable threats to more complex challenges. Running in tandem with HMIC's reviews of Public Order and Civil Contingencies, the 22 forces visited were selected according to a broad analysis of threat and risk.

The lessons arising from the review apply equally to every force in the country. The passage of time and loss of corporate memory, even in large forces, are the constant enemies of perceptive and responsive policing. The results of a series of tests (see below and Appendix A), examining force clarity of policy and staff awareness, echo HMIC's findings from *Leading from the Frontline* (2008), which argues that national guidance had been accepted by police leaders but not embedded in practice, posing risks given the environment in which the service operates.

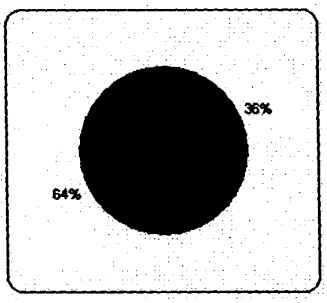
% of forces with clear definition of critical incidents



% of forces with escalation procedure



% of forces with high levels of staff awareness



Very effective measures are taken by a number of forces, both large and small, but in 14 forces (64%) staff did not have an adequate awareness of critical incidents, struggling to recognise them when they occurred, and were unclear what action should follow if they did recognise that an incident was critical.

Effective management of critical incidents flows from sound policies that are understood by everyone in the organisation, constant awareness-raising (eg, through daily briefings), and the visible leadership of chief officers and supervisors at every level. The 'effective police response' that lies at the heart of maintaining victim, family and community confidence requires an intrusive approach to post-incident review, embedded risk assessment, robust audit techniques, and a commitment to learning lessons from experience. This is the 'bread and butter' of everyday policing. If public confidence in policing is to improve, any lack of consistency and rigour has to be addressed.

Introduction

The ACPO definition of a critical incident is 'any incident where the effectiveness of the police response is likely to have a significant impact on the confidence of the victim, their family and/or the community'. This encompasses not only incidents such as murders, which may immediately be seen as 'critical' but, initially, smaller events that have the potential to escalate.

Most critical incidents are external events handled initially by police officers or staff such as [redacted] the definition also covers internal events, such as serious [redacted] police service as a whole.

The handling of critical incidents - which are frequently played out in the glare of media attention - can impact significantly upon public confidence. The public are entitled to expect the highest standards of professionalism from police forces at times of critical incidents. Failure to 'grip' such events can lead to mistakes which may be explored, years later, in courts or public inquiries.

Critical incidents can happen at any time and handling them is not the preserve of specialist units. Therefore, everyone in the force - chief officers and middle managers, less experienced front-line officers, and support staff - must be able to recognise the high risk factors in an apparently insignificant event. Such incidents can escalate quickly to critical status if they are not responded to appropriately from the outset.

As with civil contingencies, there is no shortage of guidance in this area. The NPIA, for instance, produced guidelines in 2007. The list of risk factors can never be exhaustive, but may [redacted] involvement of children, the elderly, or cases where the media's interest is immediately focussed. Racially motivated behaviour and other [redacted] factors, as are linked series offences and repeat victimisation, especially domestic abuse where there is a pattern of increasing violence.

The key elements of effective critical incident management are early identification and a professional response, allied with sensitive work in the community to maintain public confidence. These will flow from clear and effective leadership - at strategic level, where chief officers shape force culture, and in supervision and oversight on the front line. A well-run force will have a 'safety net' of procedures in which managers and senior staff monitor incident logs/daily briefings and spot potentially critical situations that have not been picked up appropriately at the outset. Speed is imperative - the importance of acting effectively in the initial 'golden hour' – before the scene goes cold or events escalate beyond control - is well established.

This inspection focused on six elements:

- Leadership and governance
- Policies and processes that comply with national standards and guidance
- Strategic direction and assessments of risk and vulnerability
- Systems for gathering and evaluating (community) intelligence
- Capacity and capability - are appropriately trained and skilled resources deployed [redacted] nts?
- Evaluation and review mechanisms

Effective leadership and governance

Chief officers are responsible for ensuring that forces are prepared – clearly informed, well trained and aware of lessons from the past - to deal with critical incidents. Ensuring grip of such incidents should be a core element of leadership in every force. A capable chief officer should 'own' – take responsibility for - critical incident policy.

However, HMIC found variable levels of commitment to this area among chief officer teams. Those forces which inspire most confidence have nominated strategic leads, usually at Assistant Chief Constable level. [redacted] In these forces, the role is more than a nominal one. The chief officers concerned have developed a critical incident management policy that is informed by threat and risk assessment, and uses intelligence and analysis to sustain the required capability and capacity. In such a culture, forces learn and improve.

In some forces, this effective leadership is complemented by good governance arrangements on the part of the police authority. This is particularly important in the area of community impact. The picture elsewhere is mixed. In five of the 22 inspected forces, HMIC found no evidence of a designated chief officer lead for critical incident policy and strategic management. Unsurprisingly, operational staff in these forces often cannot demonstrate an adequate understanding of force policy in relation to critical incident management, or are unfamiliar with what guidance is available.

Where weaknesses in strategic leadership exist, these are likely to be accompanied by the lack of a systematic approach to post-incident reviews and robust performance management. Expertise is built up through experience and exposure to risk in busier forces but also by training and accreditation of senior officers. Of those inspected [redacted] have proactively trained all or some chief officers in critical incident management.

Policies and processes that comply with national standards and guidance

National policy helps to ensure understanding, consistency and good practice; it is therefore essential that forces comply with national standards. Again, there is clear guidance, developed by ACPO and NPIA. Core elements include:

- Making up-to-date intelligence and clear analysis available – on a 24/7 basis – to those handling potential critical events;
- Effective monitoring of community tensions and impact assessments in response to critical incidents;
- Proactive management of relationships with communities, using Independent Advisory Groups (IAGs)and Key Individual Networks (KINs); and
- Routine debriefing and assessment of performance and procedures.

Some forces [redacted] can point to an overarching strategy. These are the 'big' forces, but this is not a question of resources. Others can, and should, emulate them.

National policy is of little use if it sits on a chief officer's shelf. It must be put into practice on the ground, in easily understandable form. The notion of the 'golden hour' [redacted] vividly highlights the need to respond quickly and effectively. Officers can readily grasp the point that they may never be able to recover from mistakes and omissions in the 'golden' period. Any who doubt this need only read the report on the inquiry into the death of Stephen Lawrence.

Strategic direction and assessments of risk and vulnerability

Risk in terms of community impact and concern, cost and reputation, provides a shared focus for forces and police authorities. Some forces make substantial use of 'risk registers'. Others show a limited awareness of the benefits of these risk management techniques and in some cases there is evidence of organisational complacency in officers' awareness of, and preparedness for, critical incidents.

Risk assessment should include analysis of both known and reasonably foreseeable events, as well as drawing upon community intelligence. Potential critical incidents may be anticipated, and diffused. Examples include hate crime and racially motivated incidents, child abuse, domestic violence and sexual assaults. Close attention should be paid to reports of vulnerable missing persons and events likely to generate significant public interest. This is about clear thought, not resources - it is sound, good sense. [redacted] has a Critical Incident Committee which shapes force planning, both to 'future proof' against threat and risk, and for the effective management of current critical incidents. In [redacted] Deputy Commissioner presides over weekly 'Looking Forward' meetings. [redacted] also provided strategic direction to a high standard. However, six of the 22 forces cannot produce any evidence that critical incidents are considered within the framework of the force strategic assessment. [redacted]

Systems for gathering community intelligence

In effective critical incident management, community intelligence is paramount. Information may come from other agencies or, increasingly, neighbourhood policing teams. Forces which use such intelligence effectively can identify threats sufficiently early to stem problems at source, or at least prevent any escalation. Lancashire, the MPS, and West Midlands have central units to scan open and closed sources of intelligence rigorously and many forces make good use of IAGs and KINs at neighbourhood level.

However, while forces generally have intelligence collection and dissemination processes in place, linked with neighbourhood policing teams, such processes are often not systematically overseen by the centre. Forces too often overlook intelligence retained by Crime and Disorder Reduction Partnerships (CDRPs) or other forces in the region. Furthermore, some forces do not routinely examine existing sources of intelligence, such as missing person databases or hate crime logs. These forces also tend to view Community Impact Assessments as one-off exercises rather than aspects of dynamic threat management. Incompatible IT systems add to the risk.

Some forces lack the ability to collate, analyse or assess intelligence and the overall picture of threat and risk is either incomplete or non-existent. This problem tends to be more prevalent in smaller forces which have less exposure to critical incidents, but even the smallest force cannot afford to allow a lack of focus. It takes only one badly managed critical incident to do untold damage to a force's reputation and public confidence. [redacted]

Capacity and capability

Dealing initially with critical incidents is not a specialist skill in itself – at least in the majority of cases – but a question of doing the basics well. This means handling witnesses and securing any crime scene. Where training is provided, it should be relevant to an individual's role and then properly evaluated. Those in key roles – especially control room staff taking calls from the public, or officers supervising first responders - should be a priority for training.

Command resilience is an important factor. Forces must ensure that there are sufficient numbers of officers and staff capable of performing Gold, Silver and Bronze (GSB) commander roles, particularly to handle firearms incidents. Several forces have adopted a 'top down' approach to critical incident training, with priority given to senior command skills.

National training programmes aimed at chief inspectors and the superintending ranks are well attended. Alternatively, some forces adopt a 'bottom up' approach, with the majority of training aimed at staff operating on the front line, particularly supervisors. [redacted] focussing on training for supervisory roles as part of their learning and development programme for 2009/10 There is a wide range of training models for forces to choose from, but no single approach.

More, generally, the benefit of training is not well understood because few attempts at evaluation go beyond merely achieving the initial learning objectives. Training too often fails to address the individual needs of staff. Those in the frontline - control room staff, PCSOs, constables and sergeants – reported the lowest levels of participation overall, and this is reflected in the levels of staff awareness recorded at Appendix A. The picture, therefore, is still too variable. In June 2009, the NPIA launched its new Critical Incident Awareness package, pri[redacted]ergeants, but nationally agreed training which addresses the principles of critical incident identification and early management should be integral to the learning a[redacted]t of all frontline staff, not only supervisors.

As with other key skill areas, records of those with appropriate training and expertise, or command skills, are too often inadequate. Several forces, [redacted] have invested in IT solutions. The Gold, Silver and Bronze structure is well-established. However, critical incidents requiring a significant multi-agency or force-wide response need chief or at least very senior officer representation, since this type of incident tends to pose the highest risk to reputation and public confidence.

Evaluation and review mechanisms

In six forces, critical incidents are not routinely debriefed, contrary to the ACPO standard. Some operational events, such as deaths in custody, will immediately be recognised as critical incidents and become subject to debriefing and operational review. But less obvious incidents with a cumulative impact, such as repeat offending (especially if targeted at a particular group or community) may go unnoticed unless there are mechanisms to identify them. This is often referred to as 'flagging and tagging'. However, such flagging/tagging systems can become unnecessarily complex. Some forces provide too little guidance and opportunities are lost. One medium-sized force flagged only five critical incidents in 2008, which was clearly not consistent with the size or demand profile of the force.

Conclusions

Outside those forces commended above for their good practice, the management of critical incidents is inconsistent in key areas such as strategic direction, policy compliance, quality assurance, performance review and training provision. This inconsistency derives in part from a lack of clear direction from the top. Chief officers must not step back from taking responsibility for the risk generated by poor management of critical incidents. [redacted] offer policies and strategy underpinned by rigorous analysis of available intelligence, allied with robust risk management processes. If other forces do not strive to reach these standards they are vulnerable to mission failure and damage to reputation.

An understanding of, and the ability to 'grip', critical incidents varies widely from force to force. Additionally, some forces show a limited awareness of the benefits of risk management. Where direction is lacking, this has a negative impact on the potential benefits that can be drawn from a systematic approach to post-incident review and robust performance management.