



THE HIDDEN RISK IN SECURITY OPERATIONS

When Information Isn't Understood



Bernadette Smyth

Principal Consultant, Governeering

Security professionals operate in environments where information moves quickly and decisions carry immediate consequence. Whether monitoring critical infrastructure, managing access to major facilities, responding to incidents in public spaces, or coordinating with emergency services, security personnel are constantly required to interpret information and act on it in real time.

Over the past decade, the security industry has invested heavily in technology. Surveillance systems, integrated command centres, advanced analytics and sophisticated access control platforms have significantly improved the quality, speed and availability of operational information. In many environments, security teams now have access to more data than ever before. Yet a persistent and often overlooked risk remains: the assumption that access to information equates to shared understanding.

Security decisions are still made by people. When incidents unfold, the effectiveness of a response depends not only on the systems in place, but on how clearly information is communicated and how accurately it is understood.

Communication Is Not a Soft Skill. It Is a Control.

Security incidents do not always escalate because information is unavailable. In many cases, escalation occurs because information is misunderstood, partially absorbed or interpreted differently by those involved.

During an unfolding event, information is rarely delivered through a single channel. Instead, it moves across multiple streams simultaneously – radio communications, written reports, command centre instructions, mobile alerts, visual signals and direct interactions with the public. Each layer introduces potential for distortion. In controlled environments, communication protocols can appear robust and effective. Under pressure, the conditions change: noise increases, time compresses and attention narrows.





Behavioural science shows that when individuals are operating under stress, uncertainty or emotional intensity, their ability to process complex information declines. Messages that seem clear in training may become ambiguous in practice. Instructions may be partially heard, selectively interpreted or lost within competing demands. In these moments, communication becomes a critical control within the security system itself.

The Gap Between Information and Understanding

A consistent yet under-recognised challenge in security operations is the gap between what is said and what is understood. Security personnel encounter this gap regularly. A message transmitted over radio may be understood differently by multiple team members. Instructions that require sequencing or technical language may break down entirely when delivered under pressure. These are not failures of professionalism or training. They are reflections of how human cognition operates in dynamic environments.

Under pressure, cognitive load increases and working memory becomes constrained. Individuals prioritise certain signals while filtering out others. Interpretation becomes shaped by prior experience, emotional state and situational awareness. In practical terms, this means that the same message, delivered to multiple people in the same moment, may produce different interpretations and actions.

When Good Systems Don't Deliver Good Outcomes

The security industry has made significant strides in strengthening systems, processes and technological capability. But these advancements can create a false sense of assurance if the human layer is not equally considered. Systems can generate accurate information. Procedures can define appropriate responses. But neither guarantees that information will be understood in the way it was intended.

In real-world environments, breakdowns often occur not at the point of data generation, but at the point of translation, when information moves from system to person, and from person to action. This is where otherwise well-designed operations can begin to diverge from expected outcomes.

Recognising this gap does not diminish the value of technology or process. It highlights the need to design operations that account for how people interpret and act on information under real conditions.

Strengthening Communication in Practice

Improving communication in security environments does not necessarily require additional systems. It requires a shift in how information is structured, delivered and confirmed. Several practical approaches can strengthen clarity during incidents:

Use simple, direct language.

Under pressure, clarity outperforms complexity. Short, direct instructions reduce the likelihood of misinterpretation.

Reinforce messages across multiple channels.

Where possible, combine verbal instructions with visual signals or written confirmation to support understanding.

Confirm shared understanding.

In team environments, especially those involving multiple personnel or agencies, verifying understanding can prevent divergence during critical moments.

Recognise the emotional state of the audience.

Adjust tone, pace and wording when individuals are distressed, confused or agitated to improve how messages are received.

Design communication for real conditions.

Procedures developed in calm environments should be tested against noisy, crowded and time-pressured scenarios to ensure they remain effective in practice.

The Human Layer of Security

The private security sector plays a vital role in safeguarding Australia's people, infrastructure and public spaces. As the industry continues to evolve through technology and professionalisation, it is equally important to recognise the human dynamics that shape how security operations unfold.

Security systems generate information. Procedures guide action. Technology enhances visibility. But the effectiveness of these elements ultimately depends on the ability of people to interpret and communicate information clearly when it matters most. In many security incidents, the difference between escalation and resolution lies not only in the presence of a threat, but in whether individuals involved share a common understanding of what is happening and what needs to be done.

Strengthening communication clarity is therefore not a peripheral capability – it is central to operational effectiveness. In an environment where speed, complexity and pressure are increasing, ensuring information is not only available but understood, may be one of the most important controls the industry has.

Bernadette Smyth helps organisations improve how information is communicated, interpreted and acted upon in complex and high-pressure environments through her advisory practice, Governeering. 

Interpretation becomes shaped by prior experience, emotional state and situational awareness. In practical terms, this means that the same message, delivered to multiple people in the same moment, may produce different interpretations and actions.