Risky business: why talking to the front line is vital for security and resilience

Organisations routinely recruit and train security personnel to spot and manage suspicious people and events but fail to capitalise on the pool of knowledge and experience in the workforce. The result can be defective risk assessment and ineffective mitigation, as well as staff retention and motivation issues.

In this article Andy Blackwell and John Wood, Consultancy Practice Directors of 3DAssurance look at the risks organisations take if they undervalue their security staff.

Intro

Managers are causing unnecessary risks to their organisations. Failing to talk to the front-line security officers has three very undesirable consequences.

First, it can leave them feeling disengaged or even alienated, causing retention problems and making recruitment harder. Secondly, it damages job satisfaction and motivation, which can lead to mistakes and poor results. Worst of all it poses security risks due to misinformation. In this article we look at each of these in turn.

Retention and recruitment

Organisations often regard employing security officers as a straightforward transaction. How much do I have to pay to get the skills and experience I need? How much will it cost to provide a legally acceptable working environment?

HR consultants call these the hygiene factors: they must be an adequate level to recruit staff but they are not enough on their own for the long-term retention or well-being of those staff. They address the first two layers of Maslow's hierarchy of needs, *Physical safety* and *Security of employment*.

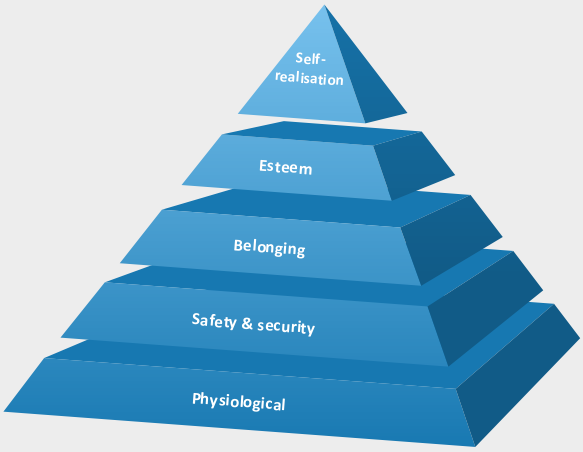
Staff well-being and retention relies on the higher levels of Maslow's hierarchy, starting with a *Sense of belonging* – of being part of the organization: "my job is important". Closely linked to that is *Esteem* – a sense of achievement, respect and value to the organisation: "People know I'm good at my job".

It's easy to see how these two Maslow needs can be fulfilled by managers, through directly engaging with the team and individually, as well as through the formal channels such as job descriptions, performance monitoring and recognition or reward schemes. How well this engagement with security staff and other frontline workers is done though, is open to question. Hardly surprising then that staff recruitment and retention is a challenge.

Maslow's Hierarchy of Needs

Maslow's hierarchy of needs was first introduced in Abraham Maslow's 1943 paper, "A Theory of Human Motivation."

There are five main levels to Maslow's hierarchy of needs. These levels begin from the most basic needs to the most advanced needs. Maslow originally believed that a person needed to completely satisfy one level to begin pursuing further levels.



The consequences are dire. Organisations with high attrition rates are losing their corporate memory.

The knowledge held by, and the experience of, those on the frontline is often underestimated, undervalued and underused by top management. To make matters worse, the pandemic, mass redundancies and industrial unrest have resulted in many companies losing vast swathes of frontline knowledge. As we can see, many industries are now struggling to recruit while their operations, services and reputation sink to new lows.

Job satisfaction and motivation

Not involving the frontline can also affect morale and motivation as these workers often know better ways of doing things and may feel undervalued if they are not included in the process.

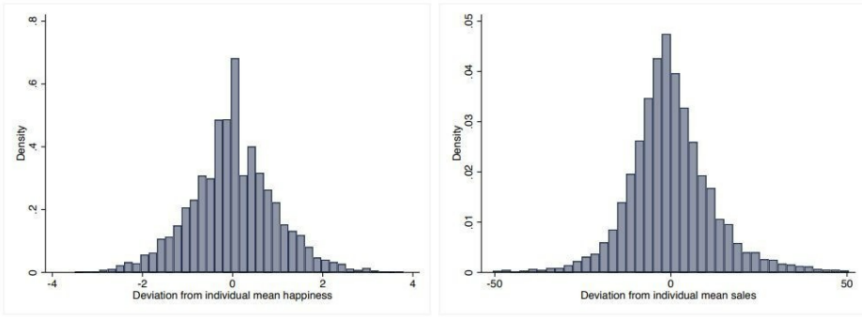
An organisation that doesn't show it cares about its people will struggle to get them to care about their work. The care must be authentic, not just motivational posters or other window-dressing. Otherwise, managers are missing opportunities to improve staff job satisfaction and well-being.

The top of Maslow's pyramid is the real game changer here: *Self-realisation* – people being able to be creative and innovative at work. This is where job satisfaction comes from: "I am encouraged to enhance the organisation's success using my skills, knowledge and ideas".

An interesting study by Jeff Sutherland, the Author of the Scrum Agile Development Process so loved by many consultants and "forward-looking" managers, discovered that the most productive teams in an organisation are the happiest. His recommendation was to ask people how happy they were in their work and what would make them happier.

Happy Employees and Productivity

Happy employees not only worked faster, making more calls per hour, but also achieved 13% higher sales than their unhappy colleagues.



(c) Happiness (within-worker) (d) Sales (within-worker)

Effect of happiness on employee productivity. Image: Social Science Research Network

It seems so obvious that consulting somebody about how they do their work would make them happier, improving their well-being and job satisfaction. Sadly few managers give their staff this opportunity, and when they do the invitation is offered to desk-based staff: the front line staff is seldom invited to that party. How many security officers really feel they can make a difference in their organisations, that their ideas are listened to?

Security as imagined – risks due to misinformation

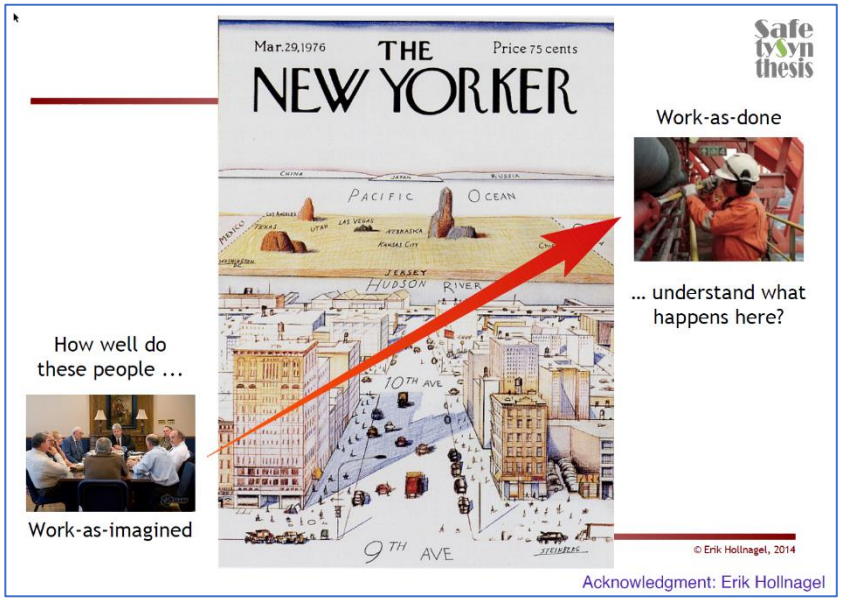
But paying insufficient attention to security officers' job satisfaction and well-being is not the only issue. Even if staff are not leaving, managers are wasting a precious resource: the knowledge and experience of the front-line security officers. Worse, they are taking risks they may not be aware of.

A challenge that many organisations face is that whilst they invariably have written security strategies, policies and procedures there is no guarantee that security is being performed as prescribed. How management imagine that security work is executed can be very different from what is actually being done, resulting in the organisation not getting a true picture of the risks it may be facing.

It is not uncommon for policies and procedures to be written by those who have no real knowledge of frontline operational practices. Worse, frontline personnel who have such knowledge are not always consulted, resulting in badly designed work and work environments, and the unintended consequences that can subsequently occur.

And those people on the frontline are the right people to ask. Managers and their consultants design the procedure manuals and think they know how the business operates; in real life the operational people know which procedures just don't work, all the shortcuts and how to get round the obstacles in the procedures. It should be no surprise that the official procedure, "the job as imagined", gets in the way of "the job as done".

So those who work on the frontline will often create adaptations to enable them to work around the badly designed work. These adaptations are not in themselves a bad thing and in fact without them the operation will often grind to a halt. The problem is that those involved in dynamic risk assessments or who are members of Risk Analysis Groups may not be cognisant of the fact that security delivery is very different from how it is specified in the procedures: their decisions are based on misinformation. This threat should not be underestimated: the Manchester Arena bombing is a sad example of what the gulf between theory and practice may lead to.



The organisation is not making the best use of its resources if it fails to consult those with knowledge of the ground truth. Honest and open discussions with front line staff and involving them in the continuous improvement process with not only help to improve security standards, but will help motivate frontline staff and demonstrate that their inputs are valued.

Some may argue that the organisation's SOPs will largely prevent this from happening, the often-large gap between security as imagined in the SOPs and security as done is unavoidable. Whilst overt and covert testing may provide an indication of performance against the processes and procedures, these are just snapshots and no guarantee of what is going on day-in and day-out.

The frontline staff are the ones who know how work is actually done, and what adaptations and workarounds to the SOPs are in place. If organisations do not recognise, do not value or make use of this valuable resource, they risk compromising their security, risk management and resilience activities.

Conclusion

Some managers are squandering a precious resource.

There was a period in the 1970s when Quality Circles were all the rage. Dr W. Edwards Deming "the Father of Quality Management" advocated putting everybody in the company to work on *constant improvement forever*. This was not about repeatedly ratcheting up performance or productivity levels, it was about asking the people that know – the shop floor – the best way of doing things.

"We cannot solve our problems with the same thinking we used when we created them" said Albert Einstein, but that is exactly how most managers in most companies these days tackle problems: it never crosses their minds get advice and fresh ideas from the frontline.

Security officers are particularly rich source of ideas because of the nature of the job. They are naturally observant, inquisitive even; they are in the habit of constant assessment of situations and acting decisively when needed; and they accumulate a lot of information from people right across the company and from outside.

Some managers really are squandering a precious resource.

3DAssurance

3DAssurance specialises in management systems for assured risk reduction, tackling the management challenges in areas such as security, risk, quality, and safety assurance. Our team combines many years of practical experience in implementing security, risk management and assurance systems, with deep analytical and strategic design expertise.

Andy Blackwell

Andy is a subject matter expert on Security Management Systems (SeMS) and a wide range of transport security matters. He provides support to government departments in the field of Security Management Systems and Threat Assessment. Andy was formerly Head of Security with Virgin Atlantic, where he was responsible for all aspects of the airline's security programme, including Security Management Systems (SeMS) implementation and development.

John Wood

John was responsible at the UK Civil Aviation Authority for developing the SeMS framework published jointly by government and the CAA. Experienced in guiding the design and implementation of effective strategic change in public and private sectors to improve operational effectiveness, John has been a lead designer of numerous governance, risk and compliance systems.