11TH JUNE 2026

THE FORTRESS

THE TOBRUK PSS LTD NEWSLETTER JUNE 2026 EDITION

PROTECTIVE SECURITY - Disruption Below the Threshold

Recent reporting from Securitas UK's Annual Intelligence Estimate has highlighted growing concerns that UK organisations are becoming increasingly exposed to disruption from threats that develop gradually and remain below traditional detection thresholds. Protest activity, hostile reconnaissance, insider risk, sabotage attempts, and drone-related threats are increasingly overlapping, creating a more complex security environment. As Mike Evans, Director of Securitas' Risk Intelligence Centre, noted, "UK organisations are not short on awareness of security; they're short on understanding." Security experts warn that many threat actors are exploiting supply chains, third-party access points, publicly available information, and low-cost technologies to identify vulnerabilities and test security measures. In many cases, warning signs emerge through online mobilisation, surveillance, reconnaissance, and pattern-of-life observation before any direct action takes place. Organisations are encouraged to strengthen early warning mechanisms, improve cross-functional awareness, and adopt intelligence-led approaches to support more informed security decision-making.

TECHNICAL SECURITY - Hybrid Model for UK's CNI

As threats become increasingly interconnected, security specialists are calling for a more integrated approach to protecting the UK's critical national infrastructure. Traditional security models often separate physical security, cyber security, and airspace monitoring, creating gaps that sophisticated threat actors can exploit. A growing focus is now being placed on intelligence-led security systems that combine access control, perimeter protection, drone detection, and continuous monitoring of IT and operational technology environments. By collecting and correlating data from multiple sources, these systems provide organisations with a more complete understanding of emerging risks. This shift towards converged security shows how technology continues to adapt to an evolving threat landscape.

CYBER SECURITY - Nationwide Cyber Warning

The UK Government's Department for Science, Innovation, and Technology (DSIT) has warned businesses that artificial intelligence is accelerating cyber threats, making attacks faster, cheaper, and easier to scale. In a recent open letter to business leaders, ministers highlighted how AI tools can now identify software vulnerabilities and generate exploits at speeds that would have been impossible just a year ago. Despite these advances, the weaknesses most commonly targeted by attackers remain largely unchanged, including unpatched systems, weak credentials, and poor cyber governance. The Government has urged organisations to review cyber risks at board level and make greater use of available cyber resilience resources. The warning serves as a reminder that cyber security remains a business-wide responsibility rather than solely an IT issue.

PERSONNEL SECURITY & INSIDER RISK - The Insider Risk Challenge

New research from the UK's leading fraud prevention service, Cifas, has revealed concerning attitudes towards insider-enabled fraud among UK workers. Their study found that around 1 in 8 employees either admitted selling company login credentials or knew someone who had done so within the past year. The findings become even more concerning among senior personnel. The research found that this figure rose to 32% among senior managers, 36% among directors, 43% for C-suite leaders, and 81% for business owners. Cyber criminals are aware of this and actively seek to recruit individuals with legitimate access to organisational systems, providing a trusted route into networks and sensitive information. These numbers show the need to strengthen security cultures in the workplace, as well as improve targeted training and access governance.

UK CRIME - Protecting Retail Workers

This month, the Government has introduced a new standalone offence for assaulting retail workers as part of the Crime and Policing Act 2026, reflecting growing concern over violence faced by shop staff across the UK. The offence carries a maximum penalty of six months' imprisonment and/or an unlimited fine, with courts expected to consider Criminal Behaviour Orders for offenders. The legislation also removes the perceived immunity surrounding shop thefts involving goods valued at £200 or less, ensuring all offences are treated as general theft and investigated accordingly. The changes signal a tougher approach to retail crime and greater recognition of the risks faced by frontline retail workers, many of whom continue to experience intimidation while carrying out their duties.

01245 520254 www.tobrukpss.co.uk contact@tobrukpss.co.uk

THIS MONTH'S SPOTLIGHT: Philip Grindell - Founder Defuse Global

Philip Grindell is a former Scotland Yard detective and the founder of Defuse Global, an advisory practice that helps prominent individuals and families stay safe from stalking, fixation and targeted threats. His work runs in two directions: reducing the personal information that makes people easy to find and target in the first place and reading the behaviour behind a threat once a concern arises. After the murder of MP Jo Cox in 2016, he built the UK Parliament's threat assessment team — work that went on to identify and stop a planned attack on another MP. Trained by the US Secret Service psychologist Dr Robert Fein, he is now one of the UK's leading authorities on how threats against public figures develop, and how they can be prevented. He is the author of Personal Threat Management and one of fewer than 300 Chartered Security Professionals worldwide.

What early warning signs relating to an obsessive or fixated individual risk are most often overlooked?
Philip explained that one of the clearest indicators is a change in behaviour. What may begin as a seemingly harmless attempt to engage can gradually develop into persistent and unwanted contact across multiple channels. While individual interactions may appear insignificant in isolation, repeated attempts to communicate through different platforms can indicate an emerging fixation.
"They may start by engaging on one social media platform, but then suddenly they are communicating on multiple platforms, emailing or phoning. That should be seen as a red flag."

In your experience, what behaviours most often precede a serious security incident?
According to Philip, serious incidents rarely occur without warning. Many follow a recognisable path beginning with a grievance before progressing towards planning and preparation. Warning signs can include hostile reconnaissance, testing security measures, repeated visits to locations of interest, or acquiring the means to cause harm.
"The dangerous moment is when someone stops complaining and starts preparing. That change is the one that matters."

What piece of security advice do you give most often?
Philip's advice is simple: trust your intuition and report concerns early. Small behavioural changes or unusual interactions may not always justify immediate action, but they should never be ignored. Effective threat management often depends on recognising and documenting concerns before they develop into something more serious.
"Almost every serious case I have worked on began with someone having a quiet feeling that something wasn't right — and then talking themselves out of it."

TOBRUK PSS LTD UPDATE

May was a highly productive month across our project portfolio. We progressed a key electronic security tender for a multi-system project in Kent, successfully completing the evaluation phase and moving through to client presentations. In parallel, we began preparations for a second security services tender, working closely with the client to review and strengthen their existing security services specification.

We were also delighted to secure a new engagement in Leicester, where we will be delivering a bespoke scenario-based desktop exercise for a new client. Alongside these larger projects, we continued to roll out our online Protective Security Assessments. These have proven to be an excellent first-step solution for organisations engaging with us for the first time, providing valuable insight into their current security posture.

Danny Moody CSyP, RISC

If your organisation needs support/advice regarding any of the topics discussed within this months newsletter or from within our range of Protective Security services please reach out using the contact details at the bottom of the page.