



Editor's Note

BY JOY FINNEGAN
EDITOR-IN-CHIEF

MURKY WATERS

The world is treading in murky waters these days with multiple geopolitical conflicts raging, elections looming and radicalism on the rise. What is the way forward and through these painful, inexplicable conflicts? Is there a way forward? I don't consider myself a pessimist or an optimist but a realist. However, I do have faith in humanity and that we will eventually find ways to, if not resolve our differences, then to learn to agree to disagree in a healthy way. So, I am optimistic that we can find ways to coexist peacefully on this beautiful planet we call home. But as a realist, I know there are no easy answers and to move forward, good fences are needed (both literal and figurative).

In this issue we have returning to share his views, Philip Baum, former editor of Aviation Security International and currently visiting professor of aviation security at Coventry University and managing director of his own company, Green Light. At the end of last year, Baum explored the aftermath of the October 7 Hamas attacks against Israel, where 1,200 men, women and children — including 46 Americans and citizens of more than 30 countries — were killed, and their impact on transportation security. You can read that piece in our Winter 23/24 issue.

In this issue, Baum takes a look at the threat to transportation security (focusing on aviation, specifically), from six specific areas. Those areas include industry insiders; operations in/over conflict zones; the intentional hijacking and/or bombing of aircraft/airports; inadvertent carriage of explosives on board aircraft; disruption due to protests; and unruly passenger

incidents as a result of conflict between passengers and/or crew.

Baum acknowledges the seemingly impossible task of ending the conflict and at the same time helps bring focus to the things we, as transportation security professionals, can do to improve the safety of the traveling public. To that end, we also have stories in this issue looking at areas we can control and in which we can make improvements. His story begins on page 14.

Writer Mark Robins explores explosive detection systems and the crucial role they play in ensuring public safety by preventing these kinds of attacks. The requirements for fast, consistent and reliable detection that is economical and easily deployable are hard to meet but there are companies using technology to make efficient detection possible. Explosive detection has evolved from basic X-ray and metal detectors to advanced systems utilizing AI/ML, radiofrequency (RF) waves and Ion Mobility Spectrometry (IMS). He spoke to leaders in the field to see what they offer and what is coming. His story starts on page 22.

Next, we take a look at computer-based training for security professionals. Their training will determine the quality of their work, and we rely on these screeners to stay vigilant to anything that could be found artfully concealed in the thousands of bins and bags they review weekly. These training programs are used by major international airports, national authorities and security companies to help their baggage screeners get and stay proficient in detecting cleverly hidden contraband. Companies are using multiple methods to keep online students engaged,


motivated and that enhance retention. Customization is also a key element. Learn more starting on page 26.

We also have an excerpt from a new book called "ZERO POINT FOUR," a new book exploring how the U.S. ended up with less than 0.4% of the ocean-going commercial ships on the seas and what it should do to correct this weakness.

This work looks at five principles: national, economic, energy and food, climate, and workforce security and the implications of this stark truth from a security perspective. From shortages in military support vessels to threats against U.S.-dollar-denominated trade, and from insufficient numbers of U.S. mariners for food and energy security to the urgent need for climate-resilient maritime operations, the book breaks each issue down to its root causes. We will be featuring excerpts from the book's introduction in this and future issues. See that excerpt on page 32.

Next, as you may have heard, cyber hackers are using every tool at their disposal to attack the transportation industry. Writer Karon Warren gives an update on cybersecurity and how cyberattacks are up 74% since 2020 and explores how the transportation sector can improve their cybersecurity resiliency. One key: knowing where the vulnerabilities are.

Finally, we have a look at perimeter fencing. Fencing can be low tech or high tech. There are new technologies that can help keep intruders out. Check out the latest in this roundtable discussion on perimeter security.

Hope you enjoy this issue - thanks for reading. Wishing you all the best as we enter the busy holiday travel season. 



The Role of ‘Security Testing’ in Assured Protection



The consequences of failed security provisions are evident in the world around us. The rise in terrorist attacks and major incidents in recent years demonstrate the critical need for effective security provisions to mitigate threats and protect the public. The effectiveness of these security systems, however, is not a constant guarantee and as a result, the systems and processes in place must be routinely tested and assured to review and mitigate risks that could exploit any vulnerabilities.

The role and benefits of security testing through quality assurance are multi-faceted. For organisations who are investing millions of pounds in equipment, resources, and complex operations, they must be confident that the investment mitigates those very risks the security provision was designed to deter. For many businesses, it is too often the case that they only discover their system is insufficient when it is subject to an attack, which is far too late. Robust quality assurance minimises this occurrence and instead pre-empts any late identification of weaknesses in security systems or processes.

Author:

Paul Mason
*Founder and Director
at Redline Assured
Security*

It is critical that security testing and quality assurance operations are routinely implemented to also assess the effectiveness of emergency response and protection measures. The entire security system needs to be analysed; this should include aspects that security is applied to, such as people, vehicles, access control, CCTV, patterns of life and infrastructure, as well as the relevant response options, communication protocols, and use of external agencies. When carrying out the assessment, metrics should be aligned with the organisation’s security objectives to provide a clear picture of the entire security ecosystem and provide early indication of current and emerging vulnerabilities therein.

A level of independent review is required to ensure thorough verification of a system’s effectiveness. Covert and overt testing are highly successful methods of quality assurance because it identifies underperforming trends and their causal factors, based on progressive and

accumulative security testing metrics that are collected on a regular basis. Whilst an organisation can identify risks and vulnerabilities during an audit, an independent quality assurance provider can take a holistic view and provide a broader illustration of ongoing issues and make recommendations for improvement based on vast experience, known industry trends, best practice and known vulnerabilities as well as proven and emerging threats.

In addition to the critical role security testing has in ensuring robust quality assurance, it is simultaneously a catalyst for improved attitudes towards and understanding of the purposes of security. Repeatable training removes complacency among security personnel by highlighting the gaps in capabilities and provides a clear course of action to improve performance. This can include ongoing upskilling and knowledge sharing of the latest behavioural detection techniques, upgraded technology, like 3D CT scanners, or changes in legislation.

By introducing a maintained programme of testing and feedback, the rise in employee engagement will ultimately result in a better security culture that is embedded within the organisation.

The role of security is to mitigate risk and prevent incidents from taking place. Without regular testing, the effectiveness of a security system is left to chance and vulnerabilities are only identified when it is too late. Redline Assured Security have a dedicated team of quality assurance operatives who routinely conduct over 20,000 independent tests a year, providing objective data upon which appropriate action can be taken to continually improve security measures. By implementing this practice, it will result in better outcomes for all.

Find out more about Redline Assured Security’s quality assurance service at sales@trustedline.co.uk and by visiting www.trustedline.co.uk