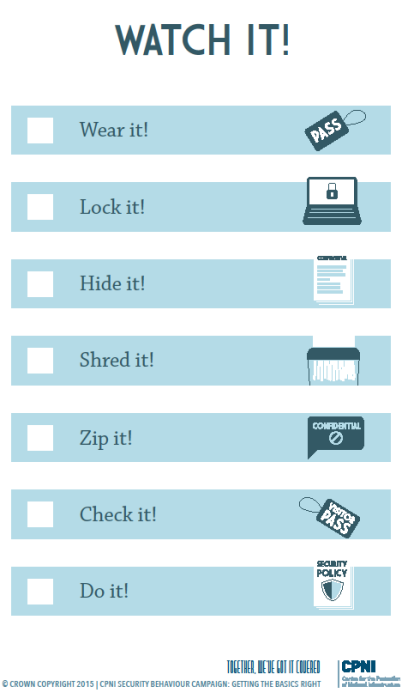
Department for Transport

An effective security culture in aviation as we recover from COVID-19

The COVID-19 pandemic has severely impacted the civil aviation industry across the world. Whilst appropriate authorities and regulators must be mindful of the constraints on the industry as it recovers from the crisis, **ICAO's Year of Security Culture 2021** presents an opportunity to encourage the industry to **build back better**. Particularly by reinforcing the importance of effective security behaviours in a returning workforce. In broad terms, building an effective security culture is an opportunity, and shouldn't be viewed as a cost or burden. At its best, it is the creation of a more effective and informed environment within which security staff and stakeholders across an airport campus can operate within.



A CPNI poster. More available here.

Amongst other issues, COVID-19 has meant that the aviation industry has had to take some difficult decisions with regard to staffing. In the UK, and many other jurisdictions, this has led to a temporary scaling down of aviation operations, often involving furlough or considerable periods of staff being out of work. As the industry recovers, it is important that organisations reorient their staff and reinforce essential security behaviours.

Further, there is no reason to believe that COVID-19 has reduced the attractiveness of aviation as a terrorist target. In fact it is likely that disruption in the sector has exposed new **vulnerabilities** and **risks**. For example, financial difficulties caused by the pandemic might make employees ('insiders') more susceptible to coercion or exploitation by threat actors. The economic uncertainty in the sector, and the consequential job security issue for employees, will have undoubtedly caused anxiety, and possibly disaffection, amongst employees. These feelings can often be a gateway on the path to becoming an insider. One way to meet these new challenges is to ensure the importance of security culture is stressed and organisations explicitly promoting good behaviours in aviation as the sector recovers.

The view from the UK

The UK's Centre for the Protection of National Infrastructure (CPNI) champions the maintenance of effective security behaviours as a vital part of addressing the threat faced by our transport networks and critical infrastructure. Drawing on the latest academic work in the fields of behavioural change and change management, the CPNI developed a pragmatic **framework** to improve security behaviour. This includes their own experiences in facilitating **practical security culture campaigns** and **programmes.**

From the UK's perspective, security culture is an indispensable tool in meeting the demands of protective security operations. International standards, domestic regulation, and the latest

technological solutions are all important. However, without a motivated staff, supported by a robust security culture, to implement these measures, a security operation could be vulnerable.

Framework to changing security behaviours

The CPNI's five-step framework, often referred to as the **5Es**, is outlined below:

- **Educate why:** Employees are less likely to adopt good behaviour if they are uninformed of an organisation's vulnerabilities, threats and the severity of the consequences. Employee education could take place through intranet articles, threat updates, case studies, and regular briefings. Security behaviour knowledge could even be integrated into performance appraisals.
- **Enable how:** If employees aren't provided with the appropriate information, training, advice and support they may not know what security behaviours are expected of them. Or even how to conduct these behaviours. Interventions which could better enable employees include security refresher courses, hand-outs, e-learning initiatives, and security-specific events.
- **Shape the Environment:** Employees should have the resources they need (e.g. equipment, materials, people); the physical opportunity (e.g. space, time, access); and the social opportunity (e.g. peer pressure, leadership, support) to demonstrate desired security behaviours. The environment can be improved by a robust redesign of security policies and IT systems, senior personnel leading by example, training and induction courses, visual aids and reminders, and correct equipment.
- **Encourage the action:** Encouragement is essential to sustaining any changed behaviours. If employees receive little or no feedback when trying a new behaviour, or they associate the behaviour with a negative experience, they may be less likely to perform the behaviour again. Tools to encourage the right action include: clear security breach policies, employee incentive schemes, acknowledgement and thank you messages for good behaviours, and corporate updates on security performance.
- **Evaluate the impact:** Organisations and airports should assess the extent to which the time, resources and costs involved have had a positive effect on protective security. And whether improvements or modifications in the approach are required. Evaluation can be done in a number of ways, including: staff surveys, focus groups, IT monitoring and records of security breaches.

In seeking to improve security behaviours within your organisation and at your airport/s it is recommend you consider these elements.

The wider benefits

Time and resource invested in developing good security behaviours also provide benefits in tackling some of the other challenging issues facing civil aviation.

On countering the threat from hostile use of unmanned aircraft, safeguarding cyber infrastructure, or mitigating the risk to air freight operations, an effective security culture can form a crucial part of our response. In the wake of the Gatwick incident, airports in the UK developed multi-layered approaches to countering drone misuse. These measures included greater security awareness amongst staff on

the airport campus and residents in local communities. For example, the introduction of "drone hotlines" for the airport community, to report sightings and improve on-the-ground intelligence.

A CPNI poster. More available here.

The benefits are clear. The global aviation industry has a long and proud tradition of prioritising safety, making it the responsibility of all stakeholders and all employees. We should aim to place security on a similar pedestal, as a fundamental concern of all involved in the aviation network. **ICAO's Year of Security Culture 2021** is an ideal opportunity to build back better security behaviours amongst employees and partners. ICAO has published incredibly useful tools, such as the Security Culture toolkit and the Security Culture Campaign starter pack, which can help guide national and organisational conversations. The UK looks forward to working with ICAO, industry and all member States to make the year a success, and to help embed robust security cultures in aviation systems around the world.

Author Details

Dr Rannia Leontaridi OBE FRSA, Director General of Civil Aviation
Department for Transport

Rannia joined the UK's Department for Transport in 2020, to be the new Director for Aviation and the Director General Civil Aviation for the UK. Over the last three years, Rannia was the Director for Business Growth, leading the UK Government's policy on entrepreneurs, small businesses, but also new and emerging high growth and technology businesses. She devised and implemented the UK's first Artificial Intelligence (AI) strategy and secured an AI sector deal in a partnership between the private sector, government and academia of £1bn. She created and became the first Director for the Office for Artificial Intelligence for Her Majesty's Government and led the Industrial Strategy Grand Challenge on Artificial Intelligence. Prior to her time in the Department for Business, Energy and Industrial Strategy, she led teams in the Cabinet Office, the Prime Minister's Strategy Unit, and the Department for Environment, Farming and Rural Affairs in policy, strategy and commercial roles. This included leading the development of more than 100 employee-owned private sector businesses, and Rannia was the Co-Founder and Director at Crown Hosting Data Centres, a joint venture between the UK Government and Ark Data Centres. Rannia started life as an entrepreneur and later became an Assistant Professor in Economics. She received an OBE for public service in 2016, is a Carnegie Scholar in Economics and a Fellow of the Royal Society for the Arts. Rannia is married with one daughter, loves to travel, and is a runner, and enjoys craftwork in her spare time.