Security Culture and Human Factors

Article by Ms. Michelle Salgado Ferreira Arcúrio, Civil Aviation Regulation Specialist, Brazil

Based on the practical alignment between the technical and the academic perspective, this article seeks to present to the civil aviation community an opportunity to debate and maximize security culture. The article presents questions for reflection, general security culture best practices and strategic security guidance for all.

Introduction

Aviation measures to ensure the industry's protection against intentional threats have been constantly improved. They have encompassed a combination of human, material and procedural resources.

Human resources i.e. staff, are considered the weakest link in this 'chain'. However, given due attention, they can become the **strongest link**, or even the most fundamental element of the security system, in order to promote a positive security culture.

Security culture is a set of norms, beliefs, values, attitudes and assumptions. It is represented through our decisions, behaviors, speeches and thinking. It is also represented in our security standards, documentation, and quality control activities.

"Culture" seems to be an abstract issue, but it is not. Due to the security relevance, it is expected that all involved in an organization's performance (decision-making, resource allocation, formal and informal rewards systems) would reflect that by developing a security culture mind.

Aviation Culture: Safety and Security

The promotion of an effective security culture in aviation is critical to achieve good security outcomes. A question that emerges in this point is: how relevant is the need to specify security culture? Why do we not consider it as simply "aviation culture"? Is security culture the same as safety culture?

Safety

Safety is concerned with the normality of the operation, meeting predictable patterns. It is based on previous studies. Its results seek to mitigate vulnerabilities already known (e.g., aircraft engine failure, staff fatigue and misunderstandings, as mentioned by PETTERSEN & BJØRNSKAU, 2015). Additionally, it aims to **anticipate identified**

problems in its operational reality or those shared by other States as best practices or lessons learned.

Security

On the other hand, security has had the function of **preventing the unknown**. What differentiates them then? Security must prevent threats against civil aviation, in addition to preventing terrorist attack attempts, so the intention is key. In order to succeed, it is imperative to develop intelligence activities, address security hypotheses and achieve a mentality that security professionals do not innately possess. Ultimately, it is expected that the procedures will be continuously improved in order to become applicable to future threats not yet imagined. As highlighted by Pettersen & Bjørnskau (2015):

> (…) *security risks are generally related to a **potentially unknown external actor** that, for the purposes of creating terror, might carry out random attacks. In this respect, whereas **safety is organized to deal with internal threats**, **security's primary target is external**. In this case, the goals of safety and security are different in the way they relate to **two very different types of protection**. As threats are internal, the effects of **safety measures will sooner or later become known**, and it is possible to judge their suitability against how well they perform. For security, however, an **event against which security measures can be evaluated might never happen**. This makes the goals as well as the institutional logics of protection between safety and security very different".* (adapted; emphasis added).

It is our responsibility not only to **learn from data historical series.** But to **learn from** what stakeholders teach through their **successes and failures**.

It is also a challenge to be **ahead of the threat**, due to the most varied forms of attack, technologies and vulnerabilities that can be exploited in civil aviation.

Connecting the Dots: from strategic to operational staff

Whatever the job post, everything that the human element does and thinks can either reinforce a security layer or maintain it. However, it can also both compromise and generate vulnerabilities. That is the reason it is challenging to civil aviation authorities thinking and acting collaboratively with other stakeholders (in terms of duties and competencies).

If there is no full alignment and validation from the strategic to the operational level, a link in the culture chain could be broken. And effort to form and foster a culture of security will be innocuous. **It is important that a strong security culture is developed from the top management across and within every organization**.

A robust security culture should reach leaders. It should transform decisions into standard operational procedures and be represented in the operational context. Dealing with pat down procedures (during pandemic situations) and rush hours in airports, whilst maintaining international aviation standards and developing a multidisciplinary vision, besides **human factors**[1], is a part of the job reality.

---

[1] Human factors is the name of an engineering profession that focuses on how people interact with tasks, machines or computers, and the environment, with the consideration that humans have limitations and capabilities. Often, human factors will study the human within the system to ensure that we understand the limitations of the human within the current structure, product, or process (DOE STANDARD, 2009).

For this reason, the crucial role of the human element in the system is noted, whether it is in strategic positions or in operational activities, such as the screener. Whatever is the job position, the impact of each activity on the system is notorious. How the dots connect!

A good security culture atmosphere is beneficial for promoting security awareness and surveillance. Thus, everyone consciously complies with security regulations and actively detects potential risks. Everyone reports suspicious behavior and exchanges information over time, based on mutual trust. And everyone actively implements preventive measures (ZHAO, SHI & ZHANG, 2016). **Raising awareness of security culture matters**. How this would be reflected in the operational level is still challenging, nonetheless, it is our duty.

Security Culture Challenges: The Security Officers

There are some challenges for the effective establishment of a positive security culture. One of those is the security officers' career. Despite playing a critical role in the aviation system there is usually no solid career prospects for security officers, along with low social recognition, low wages and high turnovers (SALTER, 2007).

Indeed, as mentioned about screeners: "*They come, work for a short time and then leave*" (DE GRAMATICA *et al*, 2016).

Therefore, there is low organizational identity, security awareness training with short-term effects and a high employee turnover. These factors decrease the quality of the provision of security to a level that can increase the risk of violations to the system and, thus, threaten international security (LEESE, 2015). Contracting practices for airport screening process (third-party) exposes the provision of security to a highly competitive market in which the price is the dominant criterion. This then turns screening operations into low-cost labor.

Every time an experienced screener leaves due to the turnover, the formation of security culture begins again. Someone needs to take over and replace. It is a continuous cycle that requires reflection and decisions.

The difference between experienced staff and beginners lies in their level of knowledge and whether they are facing familiar situations (Reason, 2009). Security often boils down to an individual decision, made under time constraints of high passenger throughput. It then appears reasonable that this decision should be made by an experienced, well-trained and highly motivated security officer (LEESE, 2015). It is for no other reason that the study of errors and human factors in airport security and screening operations, in a security culture perspective, has been explored in Arcúrio *et al* (2020).

Overcoming Challenges

Strategies for overcoming Security Culture challenges:

a) **Putting into practice** the *ICAO Security Culture Toolkit* and the *ICAO Security Culture Campaign Starter Pack* (ICAO, 2020). It has to be a high-level management commitment. Strategic and political decisions impact the operational ones (they are latent in the system, as mentioned by REASON, 2009). Transform words into actions.

b)   **Adjusting and improving recruitment, selection and training process**. It has a positive impact on the turnover reduction. It valorizes and prioritizes the security experience. Also implement a job profile analysis. If the type of contract is third-party, set the minimum requirements so the screening checkpoint supervisor needs to have at least two years of experience (in the last five years) as a security officer, for example. Actively participate on the recruitment and selection process, having the final word in hiring staff. Or establish a quality control protocol to ensure company hiring best practices. Protect the "need to know principle" as security encompass sensitive information.

c)   **Establishing a method**, such as a non-punitive and anonymous **reporting systems** to get important data (know the operational reality and what staff are seeing, including internal threats). Human factor risk management is another example that could provide a model for organizational reorientation. This is through effective security culture in the implementation of procedures, roles and responsibilities and a continuous self-assessment process (ARCÚRIO *et al*, 2020). Establishing periodicity and structure for security culture studies, adapting to the cultures and States procedures for, e.g., composing quality control criteria and/or to be one of the variables in decision programs, such as "One-Stop Security".

d)   **Analyzing technical and statistical data.** Researching and mapping is important, along with cross-checking and comparing data to check where action is needed. Looking at isolated data leads to biased interpretations and it does not give the opportunity to see the global picture. A recommendation is to combine security test results with organization training feedback and data from internal audits and those carried out by the authority. Besides that, assessing security culture over time is required. Establishing a comparative historical series for all data is useful. If possible, contributing to the academia by writing and discussing results.

e)   **Sharing methods and experiences**, whether successful or not, so States can have the lessons learned available. Creating collaborative groups and intensifying collaboration with States and industry in supporting efforts to promote security culture in the greater aviation community is useful.

f)   **Valuing Security officers work.** It is important to watch over our aviation security professionals. This will help to transform the security conscious into plans, decisions and practical actions. It will also provide a comfortable place to work and rest. Plan and enforce career structure, even on third-party contractors. When you take care of them, you take care of all processes.

g)   **Listening.** Suggestions from technical and operational staff are more than welcome. Take time to do it periodically. The reporting system alone is not enough. It is

necessary to hear, know and understand staff demands and operational problems. This provides inputs for workplace suitability, quality control and certification criteria, and generates appreciation for the security officers. It makes them feel part of the process. This creates alignment, it connects the dots. A "learning culture" is also necessary to draw and to implement the necessary changes (MEARNS *et al*., 2013). Being positive and paying attention to security briefings, even though they are questions related to queue pressure *versus* technical accuracy, is a good way, for instance.

h)   **Creating reward systems**. Promoting opportunities for the participation of security officers in training events (in addition to regular training) and developing gamification strategies (scores, professional highlights, small prizes, such as adding the minutes to the break time or providing a special snack) are valuable. Adding benefits, seeking partnerships with health, dental, life insurance and travel operators, discounts for purchases inside and outside the airport, school discounts, partnerships with universities, etc. should be considered. Whenever possible, **combining the wage with other benefits** brings appreciation for the job, making it more attractive and decreasing turnover.

i)   **Acting immediately in vulnerability situations** to not spread undesirable behaviors. Recognize identified problems, including latent ones, that arise from decision makers (e.g.: workstation design, standards operational procedures). If there are no interventions, behaviors that put aviation at risk or that bring vulnerabilities to the system can be recurrent and become a collective mental programming over time. In other words, they will become part of the organizational culture (ARCÚRIO *et al*, 2020).

This is not an exhaustive list of practical and inexpensive actions. Also, it would not be a burden or compromise the budget of stakeholders. Instead, those strategies may in fact allow everyone to exercise responsibilities and roles to promote an effective and sustainable security culture.

Final Remarks

Human resources are key to success in developing and sustaining a strong and effective security culture in aviation, from the strategic level to the operational one. The system builds in human decisions, beliefs and technical field expertise, whether in workplace design or carrying out audits, testing, inspections and writing standards. It can be difficult to build a robust security culture. But it is more than a great challenge for technicians and researchers in the sector, it is our responsibility.

It is important to note that this is a personal manifestation on security culture. The article does not necessarily reflect the ANAC's official position.

References:

ARCÚRIO, M. S. F., PEREIRA, R. R. D., & de ARRUDA, F. S. (2020). *Security culture in the screening checkpoint of Brazilian airports*. Journal of Air Transport Management, 89, 101902. doi:10.1016/j.jairtraman.2020.101902.

DE GRAMATICA, M., MASSACCI, F., SHIM, W., TURHAN, U., & WILLIAMS, J. (2016). *Agency Problems and Airport Security: Quantitative and Qualitative Evidence on the Impact of Security Training*. Risk Analysis, 37(2), 372–395. doi:10.1111/risa.12607.

DOE Standard (2009). *Human performance improvement handbook volume 1: concepts and principles.* US Department of Energy AREA HFAC Washington, D.C. 20585, available at http://www.hss.doe.gov/nuclearsafety/ns/techstds/standard/hdbk1028/doe-hdbk-1028-2009_volume1.pdf (accessed on 30 November 2020).

ICAO, International Civil Aviation Organization (2020). https://www.icao.int/Security/Security-Culture/Pages/default.aspx. (accessed on 28 November 2020).

LEESE, M. (2015). *Governing airport security between the market and the public good.* Criminology & Criminal Justice, 16(2), 158–175. doi:10.1177/1748895815603772.

MEARNS, K., KIRWAN, B., READER, T.W., JACKSON, J., KENNEDY, R., GORDON, R., (2013). *Development of a methodology for understanding and enhancing safety culture in Air Traffic Management*. Saf. Sci. 53, 123–133. http://dx.doi.org/10.1016/j.ssci.2012.09.001.

PETTERSEN, K. A., & BJØRNSKAU, T. (2015). *Organizational contradictions between safety and security – Perceived challenges and ways of integrating critical infrastructure protection in civil aviation.* Safety Science, 71, 167–177. doi:10.1016/j.ssci.2014.04.018.

REASON, James. (2009). *El Error Humano.* 1ª Edición. Madrid: Modus Laborandi.

ZHAO, J., SHI, L., & ZHANG, L. (2016). *Application of improved unascertained mathematical model in security evaluation of civil airport*. International Journal of System Assurance Engineering and Management, 8(S3), 1989–2000. doi:10.1007/s13198-016-0417-3.