SECURITY CULTURE: THE GLUE THAT BINDS A SECURITY MANAGEMENT SYSTEM

Andy Blackwell, ISARR's Senior Risk and Security Advisor, examines how organisations can enhance their security and resilience by developing and maintaining a positive security culture, the glue that binds a Security Management System (SeMS).

↓

AN '*ANNUS HORRIBILIS*', BUT OPPORTUNITIES TO SOAR ONCE AGAIN

2020 will be remembered as the most devastating year in the aviation sector's history with COVID-19 related travel restrictions significantly reducing the demand for air services, and swathes of staff being made redundant as a consequence. The impact of the deadly pandemic has reaped havoc on an already challenged industry, but also created unforeseen opportunities for agile aviation organisations to adapt, reach for the skies and soar once again.

The somewhat overused slogan ‘*Building back better*’ has relevance to the aviation sector. Despite being regarded by some as political spin, it has noble origins as the term used to describe the official Sendai Framework of Disaster Recovery adopted in the UN World Conference on Disaster Risk Reduction in Sendai, Japan in 2015. From an aviation security perspective, the ‘*Building back better*’ opportunities take the form of embedding better security practices, for example, implementing or maturing a SeMS (widely regarded as a proven method of enhancing and assuring security), and aligning security with corporate strategy. Achieving this much depends on developing a positive security culture.

THE YEAR OF SECURITY CULTURE

The International Civil Aviation Organisation (ICAO) has designated 2021 as the Year of Security Culture (YOSC), and whilst it could be argued that every year should be the year of security culture, or indeed every day, the initiative will help keep security front of mind. The fact we need specific focus on the topic though suggests that whilst good progress has been made in many areas, there is still a long way to go. The significant focus on the pandemic risks distracting us from the ongoing need for robust security and resilience. It is reassuring to hear that organisations with an established SeMS have generally fared better due to their positive security culture and focus on threat and risk management, day in day out, not just on security awareness days. ICAO defines security culture as a set of norms, beliefs, values attitudes and assumptions that are inherent in the daily operation of an organisation and are reflected by the actions and behaviours of all entities and personnel within the organisation. Security should be everyone’s responsibility – from the ground up. Effective security culture is about:

- Recognising that effective security is critical to business success;

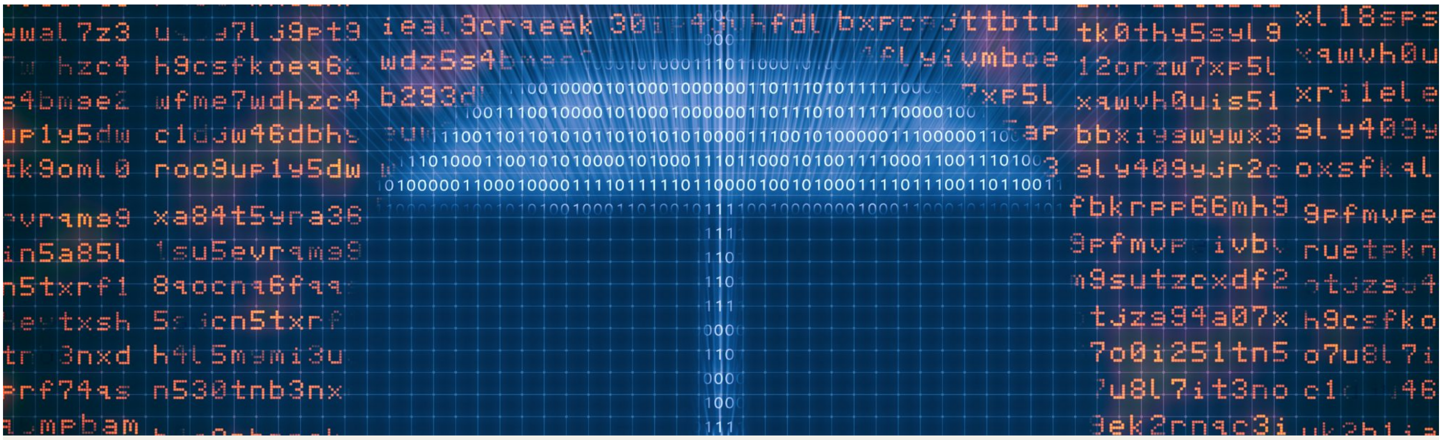
- Establishing an appreciation of positive security practices among employees;
- Aligning security to core business goals; and
- Articulating security as a core value rather than as an obligation or a burdensome expense.

In its simplest form, security culture is about '*how we do things round here*'.

THE NEED FOR HONESTY, TRANSPARENCY AND AUTHENTICITY

Whilst corporate communications invariably convey the message that security is the organisation's number one priority, closer examination of how the company actually operates often reveals a different story. In reality, whilst security is invariably a top priority, it's unlikely it would ever be an organisation's number 1 priority, and unrealistic for us to expect it to be, unless of course they are in the security business! A CEO I once worked with articulated this perfectly when he said to me "*Safety and security isn't my number 1 priority*", which initially shocked me but his further explanation allayed my concerns when he said "*My number 1 priority is to build a profitable business, safely and securely*". The CEO's statement was honest and authentic and said a great deal about the organisation's positive culture, as did the company's Values Statement '*Keeping our people and our customers safe and secure is at the heart of all we do*'.

The need for honesty, transparency and authenticity is all important when it comes to developing positive security cultures. It's counterproductive issuing a statement immediately after something untoward has taken place, saying that security is your number 1 priority if it's obvious that this wasn't the case. Moreover, if it was then the adverse event is unlikely to have occurred in the first place. Employees and indeed customers will soon identify any mismatch between a company's communication and their corporate behaviour. Honesty really is the best policy.



BEHAVIOURS REVEAL THE TRUE STORY

Corporate and employee behaviours provide us with useful insights into how mature the security culture actually is versus the impression the organisation may wish to portray. The Director who never displays his identification badge and is always asking for exceptions to be made for him sends out a signal that security is not taken seriously, or only applies to the frontline staff and not the leadership team. Management commitment is a key component of SeMS and without it security, and security culture will flounder.

The example set by one Airport CEO aptly demonstrates the value of leaders '*walking the talk*' (matching behaviour with words). Concerned about cleanliness in the terminals he issued instructions to all his staff about the need for them all to play a part in keeping the airport clean. The simple requirement being that any member of the team who saw litter on the floor should immediately pick it up and dispose of it, or arrange for it to be disposed. The CEO was regularly seen putting his words into action, picking up and disposing of litter as he went about his business. Employees seeing that the boss was literally getting his hands dirty followed suit, and the airport soon became a much cleaner place. The added benefit was that staff had a much greater awareness of, and pride in their environment. The same principle applies to security culture, the behaviours of the Senior Leadership Team will largely influence how their employees act.

The corporate response to a recent hate-crime incident where a noose was found at a construction site at Denver International Airport provides us with an example of an organisation's positive culture and zero tolerance approach to acts of bias or hate. Turner, the co-managers of the construction project together with Flatiron Construction, offered a $125,000 reward for information leading to an arrest of the person(s) involved. They also suspended work at the site for 4 days so that all workers and subcontractors could undergo anti-bias training (a prerequisite before the 550 workers could resume on the project), and hired private investigators to conduct interviews. A spokesperson for the organisation said:- "*The noose incident could have been swept under the rug but we said no more. We are going to be vocal and deliberate, and we're going to start to make a change in the industry in this project, and that was our intent. A policy is defined by words. A culture is defined by action*". The 4 day shutdown is estimated to have cost the joint venture about $1 million a day in lost production, which demonstrates that despite the significant financial impact, they did the 'right thing' by acting with integrity and signalling that hate crimes would not be tolerated at the airport. Their positive response would also safeguard them against reputational risks.

In contrast, a US congressional investigation into the deadly crashes of two Boeing 737 Max aircraft concluded that a 'culture of concealment' by the aircraft manufacturer Boeing and erroneous technical assumptions, combined with insufficient oversight by the US Federal Aviation Administration, contributed to the crashes which killed a combined total of 346 people. In addition to the tragic loss of life, the fatal crashes cost Boeing nearly £14.6bn resulting in them announcing their first annual loss in more than 20 years. Fixing their culture will take time, as will repairing the significant damage to their reputation.

RECOGNISING A POOR SECURITY CULTURE

The following non-exhaustive list summarises key indicators of a poor security culture:

- Inadequate security education

- Staff seeking ways to avoid complying with security requirements e.g. “There must be a way round this?”
- Concealment of information about breaches or concerns
- Siloed approach taken towards security – a view that security is the sole responsibility of the security team
- Reliance on the regulator to tell the organisation how they are performing – lack of assurance capability
- Low incident reporting levels
- Confidential reporting channels aren’t trusted or don’t exist
- Staff feel uncomfortable reporting security concerns
- Staff aren’t clear about what to report and when to report it
- Preventable disruptive events frequently occur
- The organisation takes a reactive rather than proactive approach to security and risk management
- The organisation behaves differently when someone is watching
- Inappropriate risk taking (risk taking is fine provided it is managed sensibly)
- When performing security activities, staff regularly take shortcuts or cut corners to get the job done
- Important security tasks are skipped or given a low priority
- Security guidance is rarely sought, or is disregarded when given
- The organisation fails to learn from its own mistakes or those of others
- Excessive secrecy about security
- Limited knowledge/information sharing
- Security is regarded as a burden to the business

DEVELOPING A POSITIVE SECURITY CULTURE

Training courses and campaigns have their place in growing a positive security culture, but are destined to fail if the content clashes with how things are actually done within the organisation. Security culture has to be much more than just appeasing words in a statement proudly displayed on the wall, or a section written in a manual that will never be read and probably end up propping open a door.

The following list summarises key steps and approaches that have helped organisations develop and maintain a positive security culture:

- Adopting the UK CAA SeMS Framework (CAP1223)
- Incorporating the lessons and best practices from Aviation Safety (as appropriate)
- Aligning security culture with company culture, values and strategic direction
- Ensuring leaders walk the talk, rather than just talk the talk. Matching behaviour with talk increases credibility and trust.
- Understanding how things are actually done within the organisation as opposed to how management believes they are done
- Explaining the ‘Why’ e.g. Why we need to comply with the organisation’s security arrangements (once people understand the ‘Why’ they are more likely to comply)
- Making security work for people, security that doesn’t work for people won’t be effective
- Implementing a Just culture approach to encourage self-reporting and the fair treatment of staff reporting security breaches, near-misses, errors and incidents
- Communicating and promoting examples of good security practices and behaviours
- Reinforcing the message that security is everybody’s responsibility and a business enabler

CONCLUSION

Security culture and SeMS are inextricably linked and a positive security culture acts as a glue that binds together the SeMS through the actions and mindset of its key stakeholders. This is particularly relevant in the context of aviation security’s Risk Assessment Groups and Security Review Boards. Achieving and maintaining a positive security culture is a lengthy but necessary process that not only protects organisations in the stickiest of situations, but creates business efficiencies and opportunities.

Many organisations who are developing a positive security culture adopt the UK CAA's Aviation Security Management Systems Framework (CAP1223) to manage and assure their security. The content of the Framework, developed jointly by Government and industry, is widely regarded as best practice.

REFERENCES: SOURCES AND FURTHER READING

UK CAA: Framework for an Aviation Security Management System (CAP1223)
https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=6543

ICAO Security and Facilitation Year of Security Culture 202
https://www.icao.int/Security/Security-Culture/Pages/YOSC-2021.aspx
Accessed 14/01/21

ICAO What is Security culture
https://www.icao.int/Security/Security-Culture/Pages/default.aspx

In the development of a positive security culture, what lessons and best practices can we take from the experience of aviation safety?
https://www.icao.int/Security/Security-Culture/Articles/An%20article%20by%20the%20UK%20CAA.pdf

CPNI Developing Security Culture
https://www.cpni.gov.uk/developing-security-culture

Sendai Framework for Disaster Risk Reduction 2015-2030
https://sustainabledevelopment.un.org/index.php?page=view&type=400&nr=2157

NCSC Growing Positive Security Cultures
https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

Noose Found Hanging At DIA Worksite; Police Investigating, Concourse Expansion Work Temporarily Stopped

https://denver.cbslocal.com/2021/01/12/noose-dia-worksite-construction-project/

Boeing's 'Culture of Concealment' to blame for 737 Crashes
https://www.bbc.co.uk/news/business-54174223

The Concept of The Information Security Culture
https://www.researchgate.net/publication/271399110_The_concept_of_the_information-security_culture

The Best Glue In The Business: Culture
https://www.humansynergistics.com/blog/culture-university/details/culture-university/2016/10/05/

FURTHER INFORMATION

If you are interested in further information about the system, would like a demo, or even arrange an initial telephone chat, you can get in touch using the "Contact Us" button below

GET IN TOUCH ✉

Location

85 Great Portland Street, First Floor, London W1W 7LT

Office Number 0203 4750 753

Subscribe

Subscribe to our newsletter to stay up to date with our most recent articles and updates.

SUBSCRIBE