Abstract

Information security breaches are becoming more commonplace. The aviation industry was historically nowhere near as safe as it is today. Having gone through a period of safety transformation, it now has an enviable safety record. Much of this is due to the safety culture framework that was implemented in response to numerous disasters. This article provides an overview of how a similar framework, adapted from the UK Military Aviation Authority’s model for an engaged air safety culture, could be employed to reduce the prevalence and severity of cyber security incidents.

Mayday, Mayday, Mayday

On 28 December 1978, United Airlines Flight 173 was en-route to Oregon. Having been given clearance to land by Air Traffic Control, the plane’s captain lowered the landing gear, yet cockpit indications showed that it had failed to engage correctly. About an hour after the plane’s crew first became aware of the problem, the aircraft ran out of fuel and crashed into a suburb in Portland. Luckily, of the 181 people onboard, only 10 lost their lives.

An investigation into the cause of this accident was conducted, as was standard practice. The investigation revealed that the landing gear had in fact engaged correctly and the plane could have been landed safely. The captain told interviewers that the fuel had depleted quicker than expected and proposed a fuel leak as the cause of the accident. In reality, his crew had informed him of the reducing fuel levels, but the captain had been so focused on diagnosing the problem with the landing gear that he had lost track of time.

What has this got to do with information security? Part of the answer to this question lies in what happened during the investigation into the crash of Flight 173. Investigators noticed that other aircraft had crashed in similar circumstances: one a year earlier in San Diego, killing all onboard, and another a couple of years prior to this en-route to Miami, killing 101 people. The root cause in every case was a loss of perception of time.

The investigators published their findings, along with a recommendation that all airline crews be taught Crew Resource Management. Considered a landmark finding, implementation of these recommendations resulted in the rate of crashes significantly declining - thousands of lives have been saved as a result. Failure in aviation is taken seriously, the value of errors is recognised as an opportunity to improve safety throughout the entire aviation industry. In aviation, errors are exposed wherever they occur.

Over the years, this approach to investigating and learning from accidents, as well as near misses and safety related observations, has resulted in the development of what the industry terms an air safety culture. Having worked extensively within the aviation industry for the past decade, I asked myself...
what could an information security culture based on similar principles look like? Before answering that question, however, two questions that are more pertinent need answering: why do we need an information security culture and what is wrong with the current approach to security culture?

Why do we need a security culture?

To answer why we need a security culture, one only needs to take a look at the number and types of security incidents over the past few years. Yahoo publicised two data breaches in 2016, one had occurred in 2013 and affected over 1 billion user accounts whilst the other happened in 2014 and affected half that number. Also in 2016, LinkedIn announced 100 million members’ account details had been exposed and Dropbox reported that 68 million users’ details had been compromised, with both incidents taking place 4 years earlier. The UK Information Commissioner’s Office fined TalkTalk, a communications provider, after a 2015 breach which was due to an unpatched vulnerability in a system acquired 6 years prior. Then there are the numerous distributed denial of service and ransomware incidents that have made national or global news. I think it is clear that the same mistakes are being repeated time and again, yet as an industry we are not learning from them.

What’s wrong with the current approach?

What, then, is wrong with the current approach to security culture? Previously proposed frameworks for establishing or discussing security culture are predominantly based around either Schein's or Detert's models of organisational culture. Schein's model focuses on the aspects of an organisation that are visibly discernable, organisational strategies, goals and philosophies, and the basic assumptions and values of employees. Detert's model is based on Total Quality Management, and therefore focuses on defining and measuring organisational change.

The security culture models based on these, however, are either too abstract or too granular. Those which are very abstract are useful contributions to the overall discussion of what constitutes a security culture but provide limited practical guidance on how to implement theoretical ideas. Those which are too granular can help when considering behaviours, actions or policies but are not easily portable between industries. What is needed is a model that is sufficiently abstract to be applicable across all organisations whilst also providing suitably concrete guidance that is relevant to each individual organisation.

A blueprint

Consider a house. No single blueprint for building a home exists. Architects design homes based on the needs of their owners, knowing that there will be various common requirements such as a living area, kitchen, bathroom and bedrooms. These accepted fundamental requirements are sufficiently abstract to be conceptualised to meet any housing design whilst at the same time being granular enough to be easily comprehended and implemented. A framework for an information security culture ought to be similar.

Whilst previously proposed models for a security culture are not adequately meeting the needs of organisations, they do highlight some common points that should be considered essential in any replacement framework. The main guidelines are that human factors are just as important as physical, procedural and technical controls, security is a sub-culture of wider organisational and national culture and that people’s underlying beliefs and assumptions influence their knowledge, motivation, commitment and behaviour, which in turn influences their actions and organisational processes. Further points to consider are that a security culture provides a long-term security strategy and should adapt to changing risks and requirements, leadership should lead by example and have upwards accountability, trust and communication must be bidirectional, and security training, education and knowledge sharing is vital.
Groundhog day

If each occurrence of the word ‘security’ in the above paragraph is replaced with the word ‘safety’ it is not difficult to imagine that each of these attributes are what would have been required across the aviation industry to identify and introduce Crew Resource Management. Major aviation disasters and their lessons are not just consigned to history books. The UK Ministry of Defence established the Military Aviation Authority in 2010, in response to The Nimrod Review. This review was a ministerially initiated investigation into the crash of a Royal Air Force Nimrod aeroplane that occurred in Afghanistan in 2006. The crash was attributed to “a failure of leadership, culture and priorities”. Similarly to previous aviation disasters, the lessons to be learned were not new and were comparable to accidents on a similar scale, such as the Space Shuttles Columbia and Challenger, the Herald of the Free Enterprise and the King’s Cross fire.

Key findings from The Nimrod Review include failing to adhere to basic principles, an airworthiness system that is not fit for purpose, an ineffective and wasteful safety case regime and a safety culture that allowed business to eclipse airworthiness. To address these key findings, four key recommendations were made:

- Adherence to new principles surrounding leadership, independence, simplicity and people.
- Introduction of a relevant, effective and understandable airworthiness regime which promoted new attitudes and behaviours.
- Defined, specific, relevant and proportionate risk cases.
- Introduction of a new safety culture.

Would it be fair to make the same comments about the approach and priority given to information security by many organisations? Some may disagree, but I believe it is a fair assessment of the current situation and that a similar overhaul is required within the information security community.

From air safety to information security

The Military Aviation Authority define air safety as “the state of freedom from unacceptable risk of injury to persons, or damage, throughout the life cycle of military air systems. Its purview extends across all Defence Lines of Development and includes airworthiness, flight safety, policy and the apportionment of resources. It does not address survivability in a hostile environment.” The standard definition of information security, which should be familiar, is the “preservation of confidentiality, integrity and availability of information”. An information security culture framework should define what is meant by information security, and a useful revised definition of information security is:

“The state of freedom from unacceptable risk of loss of information confidentiality, integrity, or availability throughout the lifecycle of a system or service. It extends across all organisational areas and addresses resilience to an attack”.

Similarly, a definition of an information security culture must be provided. An important point to note is that such a culture is an engaged culture, and is based on the Military Aviation Authority’s definition of an engaged air safety culture:
An engaged information security culture is that set of enduring values and attitudes, regarding information security issues, shared by every member, at every level, of an organization. It refers to the extent to which each individual and each group of the organization: seeks to be aware of the risks induced by its activities; is continually behaving so as to preserve and enhance security; is willing and able to adapt when facing security issues; is willing to communicate security issues; and continually evaluates security related behaviour.

Again, those with any familiarity of information security management are likely to recognise this definition as including many of the fundamental aspects of an information security management system as defined by ISO/IEC 27001.

Figure 1: Overview of the Swiss Cheese Model

Before presenting the model, however, I would like to address one final aspect that I think is useful when considering information security management. Security practitioners often talk about defense in depth. The world of safety culture has a similar concept when it comes to preventing accidents and it can be succinctly described by the ‘Swiss Cheese Model’, developed by Reason, a prominent expert in safety culture. In this model, an accident occurs when a dangerous event takes place and all the safety measures in place fail, represented by the holes in the cheeses being in alignment, as shown in Figure 1. To stop the accident from happening, only one safety measure needs to be successful - that is, a hole in one slice of cheese needs to be blocked. This model is useful to help conceptualise the goal of information security - if just one event in the chain can successfully be prevented from occurring, the entire security incident can be prevented.

A Model For An Engaged Information Security Culture

The model that follows incorporates all of the facets highlighted above, takes into consideration the seven key guidelines for a security culture and addresses the key recommendations highlighted above. An engaged information security culture consists of ‘values and behaviours’ components and underpinning components. The values and behaviours components are subdivided into five cultures: just culture, reporting culture, learning culture, flexible culture and questioning culture. The underpinning components consist of three elements: leadership commitment, open communication and an effective decision making process. Figure 2 shows how each of these elements interrelate.
A just culture means all personnel must understand that honest errors can be made. It is the cornerstone in ensuring that such errors are dealt with fairly and appropriately. However, it needs to be understood that this is not a blameless culture and deliberate violations of rules and regulations could result in disciplinary action.

In a reporting culture, open and honest reporting of information security concerns by stakeholders at all levels is essential to understand and manage the potential causes of future breaches. The understanding and exploitation of a just culture and information security management system are vital for a healthy reporting culture.

Learning followed by communication is a central part of an engaged information security culture. If lessons identified within one sphere are not effectively communicated across all areas, there is potential for undesired outcomes to be repeated. Proper investigation of occurrences and management of resultant recommendations is key to an effective learning culture, facilitated by an information security management system.

In a flexible culture, the complex and diverse nature of organisations dictates that the response to information security concerns be flexible. Rigid adherence to inadequate policies will not enable satisfactory resolutions to problems. Policy must evolve to meet challenges presented by organisational complexities.

A questioning culture is the keystone of an information security culture. People and organisations need to be encouraged to ask questions such as ‘Why?’, ‘What if?’ and ‘Can you show me?’ as opposed to making and accepting assumptions in order to achieve a strong information security culture.
It is widely accepted that leadership commitment is vital if a successful information security culture is to develop within an organisation. It is unrealistic to expect the desired culture to flourish if the leadership is not committed to it. Clear and unguarded communication of information security related information, throughout all levels of the organisation, is required if the intelligence contained within such information is going to be exploited to the full. Information security needs to be fully embedded within all aspects of an organization’s decision making processes to ensure that the security impact of any decisions is considered and understood.

Each of these elements are of equal importance. If any are omitted, the result will be an ineffective model. Many organisations already employ tools and practices within one or more of these subcultures and underlying components. However, without understanding how they contribute to a wider security culture model, their effectiveness is limited. Much like there was a need to reduce the number of aviation safety incidents all those years ago when Flight 173 and many others ended in disaster, there is a real need today to reduce the number of information security related incidents. My only hope is that it doesn’t take the loss of a life before we start to take action.

Biographies
Ashley Bye is a former Royal Navy helicopter pilot who recently embarked upon a new career in information security. Having completed his MSc in Information Security at Royal Holloway, University London, he is currently employed as the Security and Compliance Manager for Wirehive, providing hosting solutions for modern digital agencies.

Siaw-Lynn Ng is a Senior Lecturer in the ISG. Her research interests includes combinatorics and finite geometry and their applications in information security.

Series editor: S.- L. Ng