Defining and Developing a Model for an Engaged Information Security Culture

Ashley Bye

Technical Report

RHUL–ISG–2018–1

2 March 2018

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

100837572
Ashley, Bye

Defining and Developing a Model for an Engaged Information Security Culture

Supervisor: Siaw-Lynn Ng

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date:

ACKNOWLEDGEMENTS

I'd like to thank God for giving me the opportunity to pursue this Master's degree and for providing me with the resources and support to do so.

My supervisor, for your helpful and insightful guidance.

To Jo, for your love, support and encouragement throughout.

Thank you.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ASIMS	Air Safety Incident Management System
ASMS	Air Safety Management System
CEO	Chief Executive Officer
DDoS	Distributed Denial of Service
GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organisation
IEC	International Electrotechnical Commission
IoT	Internet-of-Things
ISIMS	Information Security Incident Management System
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
MAA	Military Aviation Authority
MoD	Ministry of Defence
RAF	Royal Air Force
SIEM	Security Incident and Event Monitoring
SMS	Safety Management System
SOP	Standard Operating Procedure
STOPE	Strategy, Technology, Organisation, People and Environment
UK	United Kingdom
VMHS	Virginia Mason Health System

EXECUTIVE SUMMARY

Effective information security requires more than just implementing technical, physical and procedural controls. The increasing number of security breaches and their broad impact has led to an expanding volume of research into how organisations can implement an information security culture. Legislation such as the European General Data Protection Regulation helps, inter alia, to shape national aspects of this culture. However, it is the reification of often abstract concepts at an organisational level that this research seeks to address. Unlike much of the previous literature, which utilise aspects of organisational theory as a basis for developing a model for information security culture, this report addresses the topic from the perspective of safety culture as articulated by Reason and expanded upon Haddon-Cave QC. By comparing the common requirements of an information security culture and safety critical industries such as aviation and healthcare, it argues that there is sufficient cross-over to make further comparison worthwhile. Using the United Kingdom's Military Aviation Authority's model of an engaged air safety culture as a foundation, a model for an engaged information security culture is developed. The final framework – derived from the learning of various case studies in these safety critical industries and applied to information security objectives – consists of several values and behaviours components (just culture, reporting culture, learning culture, flexible culture and questioning culture) and key underpinning components (leadership commitment, open communication, and effective decision making). Conclusions from the report show that when these components are all implemented, the benefits can include improved risk awareness and reduction, increased organisational and employee knowledge and motivation, reduced litigation attempts, and good reputational value. Whilst the focus of this project and report is primarily concerned with the security benefits from developing an engaged information security culture, it also acknowledges that components of the model can have an indirect positive impact in other business domains. The principles identified in this report could be applied to business environments today, although being based on logic and thought-comparison, further academic scrutiny would enable their refinement and promote further discussion in the context of existing research.

SECTION 1 INTRODUCTION

Since 2013, 9,011,704,027 data records have been reported either lost or stolen, which is 5,586,921 records per day or 65 every second; of these, only 4% were encrypted, rendering the stolen data useless [22]. In 2009, there were 90 confirmed breaches in the Verizon Data Breach Investigations Report [77] increasing to 2,260 in 2016 [78]. This is an increase of 2,500% in a 7-year period and does not account for incidents where breaches have neither confirmed nor reported to Verizon.

Yahoo announced in December 2016 that a data breach of more than 1 billion user accounts had occurred in August 2013. This was short on the heels of a disclosure in September 2016 concerning a 2014 breach affecting half a billion accounts [72]. In May 2016, LinkedIn [65] announced that more than 100 million of its members' account details had been exposed in a security breach in 2012. August 2016 saw Dropbox [23] announce over 68 million users' details had been compromised in a 2012 data breach. The Information Commissioner's Office [27] announced a £400,000 fine for TalkTalk after a 2015 data breach of 157,000 customers account details, resulting from an unpatched vulnerability in a system acquired as part of an acquisition of Tiscali UK in 2009.

October 2016 saw Dyn subjected to a Distributed Denial of Service (DDoS) attack by a Mirai-based botnet, causing service outages and reductions in speed for several major organisations [34]. A month earlier, the website of the security blogger Brian Krebs was subjected to a similar DDoS attack by a Mirai-based botnet [33]. The Mirai-based botnet, which almost took the entirety of Liberia's internet infrastructure offline in late 2016, and others like it are perpetuated through Internet-of-Things (IoT) devices [19].

Some of San Francisco's Municipal Transportation Agency's systems were put out of action on 25 November 2016 due to a HDDCryptor ransomware attack [21]. In February 2017, a local council in Devon had various files held to ransom after being infected by Locky ransomware [80]. On 12 May 2017, at least 16 National Health Service hospitals in the United Kingdom (UK) were forced to turn away patients due to becoming infected by the WannaCry ransomware [35]. This, however, was but a

part of a much wider, global, cyber-attack that infected computers across the globe [24].

What these examples highlight is that similar attacks are being conducted and organisations are continuing to fall foul of them. Furthermore, McAfee Labs [40] forecast that attacks on IoT devices will increase over the next two to four years. A similar forecast is made by Malwarebytes Labs [38], who also suggest similar trends in ransomware. The trend of increasing numbers of information security incidents and data breaches, and the delays between their occurrence then being discovered and reported, suggests a pattern that is unlikely to change in the near future, despite the best efforts of new controls and technologies. Rather than a purely technological approach, perhaps the solution, or part thereof, lies in the cultural approach taken.

Research into information security culture did not begin in earnest until the beginning of this century, although it remains an area that has had limited exploration and where understanding is still in its infancy [44]. Having previously worked as a helicopter pilot within the UK's Ministry of Defence (MoD), the author has experience working in an environment which emphasises the importance of a safety culture. Based on this experience, a hypothesis was developed that the principles underpinning what the UK Military Aviation Authority (MAA) calls an engaged air safety culture could be applied to information security. Accordingly, the remainder of this thesis will approach the topic from this view point.

To be able to present the final model for an engaged information security culture, it is necessary to first review existing literature relating to the subject and demonstrate the relationship between air safety and information security. This leads to an overview of the MAA model of an engaged air safety culture and an introduction to each of its underlying values and behaviours components and underpinning components, which is the culmination of Section 2. With the necessary background material in place, each of the values and behaviours components are examined in turn. Section 3 considers a just culture, Section 4 explores the concept of a reporting culture, Section 5 examines what it means to have a learning culture, Section 6 explains the idea of a flexible culture and Section 7 investigates a questioning culture. The focus of Section 8 is on the model's underpinning components: leadership commitment, open communication and effective decision making. Finally,

a complete model for an engaged information security culture is presented in Section 9 before concluding remarks are made in Section 10.

Rather than seeking to re-invent the wheel, this thesis aims to show how a model that has been used successfully in the safety industry for many years can be adapted for the benefit of information security. For this reason, each of the main sections take a similar approach: an introduction to the topic; a case study from a safety related industry such as aviation or healthcare; an analysis of the case study to determine how the concepts highlighted are applicable to information security; a case study to illustrate how these lessons contribute to an engaged information security culture; finally, a summary of the main concepts.

SECTION 2 BACKGROUND MATERIAL

2.1 LITERATURE REVIEW

It was decided that literature returned from a Google Scholar search for the phrases “information security culture”, “information security culture model” and “information security culture framework” would be reviewed prior to commencing any meaningful study. The relevance of papers for inclusion in a more in-depth review was determined based on whether they presented any models or expanded upon those presented elsewhere in literature. From these potentially applicable studies, select references were also chosen for review. The review process was aided by Pevchikh’s [44] systematic literature review of existing information security culture research that had been published between 2002 and 2014. A summary of the material deemed relevant to this thesis follows.

Studies by Schlienger and Teufel [63][64] led them to state an information security culture is formed of technical security measures supported by socio-cultural activities to embed information security into the everyday activities of organisations. It is a sub-culture within organisational culture, for which the model developed by Schein [61] can be used to deduce what an information security culture is. This model has three foundational elements: unconscious assumptions and beliefs; conscious knowledge, norms and collective values; and, interpreted creations and artefacts, which are the visible expression of the previous two factors. The work identifies culture as being non-static, evolving via a continuous cycle of assessment and either change or maintenance. An information security culture, therefore, needs to be continuously marketed to an organisation’s employees, but it must be sold as a culture that meets the corporate goals of the target organisation. To do this effectively, clear goals and objectives must be defined in a security policy and strategies must be developed for each target audience to be influenced by the policy. To create a culture, policies alone are insufficient. They must be used to guide communication, training and education, and to facilitate management to lead by example. It is proposed that only by doing these things will an organisation gain employee commitment to information security and thus form an information security culture.

In another study, Schlienger and Teufel [62] assert that human factors are often discounted in the discussion of information security, with focus being given to technical controls instead. However, this is considered unsatisfactory and a socio-cultural approach which considers humans as security assets should be taken, based on partnership, trust and appropriate use of technology. Staff should be considered as a safeguard, with hiring and training considerations forming part of the security risk assessment. As with technical safeguards, an element of residual risk will remain and organisational security policies should dictate to what level this is acceptable. Importantly, reciprocal trust between employees across all levels of the organisational structure is required to foster an effective information security culture. This culture is a sub-culture which is all encompassing and can be best defined by combining the views that every organisation is a culture and every organisation has a culture. This study suggests that a model for information security culture could be developed from safety culture, which encourages many desirable qualities. Abnormal behaviour, defined as technical and human errors and mistakes leading to security breaches and incidents, must be reported and owned up to. Such reports should be free of disciplinary procedures except in cases of malicious intent. Doing so enables a better understanding of risk. Employees need to be involved in the process and feedback systems implemented. An information security culture, therefore, must address all of these socio-cultural aspects, and be designed around business objectives and employee behaviours first and foremost.

A study by Ruighaver et al. [56] suggests that this focus on using socio-cultural methods to support technical controls reinforces a belief that security is primarily a technical function, not managerial. It therefore proposes that due to the different security requirements and overall culture of companies, security measures and policies should be bespoke and designed around the needs of an organisation rather than around the technical controls employed. Ergo, this is a managerial function because the opinion of decision makers as to the need and quality of security along with the methods used to manage it directly impacts the security practices of an organisation. Using the model of organisational culture developed by Detert et al. [15], the study makes various additional observations. Organisations often lack a long-term security strategy and tend to focus on short-term details. Motivation to achieve and partake in security activities is commonly approached from a

punishment avoidance mentality. Security, including its overarching strategy and governance, must adopt a process of continuous change to enable its evolution along with an organisation. Staff need to feel engaged in the security process, thus management should respond positively to feedback. Development and day-to-day management of security policies should be done in collaboration with all stakeholders, otherwise security measures are likely to be negated by decisions made in other business areas. A security sub-culture must be aligned to the wider culture of the organisation in its ways of working and management style, to help prevent failure of security policies. Responsibility for decisions must be assigned as part of the security strategy, and higher levels of management encouraged to assume accountability for decisions. Security practices should be aligned to external influences and changes, which includes audit and regulatory requirements as well as to the internal business environment, with processes in place to evaluate and improve strategies. For these reasons, the study considers that a single framework will not satisfy the complex requirements of an information security culture.

Employee behaviour is identified by Martins and Da Veiga [76] as a key risk that an information security culture helps to mitigate. A model is offered for a security-positive culture (where employees always process data in a secure manner to preserve confidentiality, integrity, availability and privacy), validated by Structural Equation Modelling. It is based on an organisation's management activities and policies, and employee awareness and compliance, which combine to guide behaviour. Such behaviour then becomes normative behaviour for handling information securely. It is argued that if an organisational culture does not prioritise such behaviours, employee actions will increase the risk of security incidents and breaches. To this end, the key building blocks of a security-positive culture are influenced by: information security commitment; importance; policy effectiveness; directives; responsibility; necessity; assets; monitoring perception; and consequences. By validating their model, they found that the relationships between these factors have a strong and positive influence on information security culture.

Continuing the theme of employee behaviour being one of the biggest issues an organisation has in its ability to protect information, Thomson et al. [73] propose a model that seeks to rectify this through the enhancement of employee skill, knowledge and commitment. This is done by taking the explicit knowledge of a group

of individuals and, through various stages, transforming it into tacit knowledge, or beliefs and experience. The aim being to move individuals from a state of unconscious incompetence through conscious incompetence and conscious competence to unconscious competence. By focusing on the advancement of information security knowledge and skills with training and education so that they become everyday activities, the conclusion is that such activities will enforce employee commitment to security objectives.

Another framework for an information security culture is proposed by AlHogail [1]. It aims to influence employee behaviour in achieving conformity to required security practices. It is based on the relationships between various human factors, Bakry's [3] Strategy, Technology, Organisation, People and Environment (STOPE) model and change management principles, which are combined to instil good information security behaviour for the protection of information assets. The components of the model relating to human factors are preparedness, responsibility, management, and society and regulations. The primary building blocks of the framework are based around the STOPE model, which is an acronym for strategic, technological, organisational, people, and environmental factors. Each of these relate to one or more change management principles: training; focus groups; change agents; motivation; milestones and measures; involvement; management support; resources; communication; and culture analysis.

Lack of security knowledge among employees or their unwillingness to cooperate with security policies and procedures are identified by Van Niekerk and Von Solms [43] as a significant threat. An information security culture must address these issues whilst helping to maximise productivity and minimise costs: the normal goals of a business. Research into information security culture has largely focused on the model of organisation culture defined by Schein [61], and is based on three factors: artefacts; collective values; and, assumptions and beliefs. Information security knowledge and behaviour among employees cannot be assumed, so becomes a fourth factor when considering how organisational culture relates to information security culture. Recommendations for security awareness training in information security standards fall into this category. The researchers hypothesise that such education, over time, would influence the other three factors, each of which will change in response to changes in one or more of the others. The cumulative effect

of these variables determines the overall security effect, and any changes cause the overall security culture to move in relation to a desired baseline (e.g. conformity to a security standard). The interplay between each factor impacts the desirability and predictability of the security culture in any given situation. Their adapted model of organisational culture as it pertains to information security is primarily designed to aid in reasoning about its culture. In its current state, it has limited practical value but is useful for managers to conceptualise how they might alter one variable to influence the others.

Deeming it necessary to distinguish between factors which constitute an information security culture and those which influence its creation, Alnatheer [2] conducted a review of thirteen studies. From this, seven factors are identified as an important part of any conceptual models of an information security culture: top management support; establishing and enforcing an effective information security policy; security awareness; information security training; information security risk analysis and assessment; ethical conduct policies; and security compliance. These factors form the core of the security culture, which is influenced by the wider organisational culture and aspects of national culture. These higher level cultural factors influence, rather than constitute, the components of an information security culture model.

Various definitions have been proposed for what constitutes an information security culture. The most comprehensive (via informal consensus [1][2][44]) has been suggested as:

> "*the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time*" [75].

Given that many of the above studies state that information security knowledge is integral to an effective information security culture, some literature regarding this specific aspect was also reviewed. There have been several studies of knowledge

sharing in relation to information security. They provide valuable additional insight to the discussion and are therefore summarised below.

Information security knowledge sharing is identified by Safa et al. [57] as an activity that increases security awareness whilst simultaneously reducing its cost, and includes the sharing of experiences, ideas and knowledge. Doing so helps prevent different groups from developing the same solutions to similar problems, thus freeing up resources to improve the quality of existing solutions. However, convincing professionals to share this knowledge is hard, with many being reluctant to do so owing to: confidence in ability; perceived danger of job loss; cost; subject unfamiliarity; individual attitude; and trust. Various internal and external factors influence knowledge sharing. Organisational support and trust are identified as key requirements to facilitate information security knowledge sharing and provide the necessary foundation for motivating individuals to do so.

Much focus has been placed on formal training to inculcate good information security practices within organisations, and Dang-Pham et al. [13] argue that informal knowledge sharing also plays an important role in propagating security practices. This includes sharing of experiences, ideas and knowledge, which are not always beneficial and can include dissemination of security workarounds, especially if such practices are exhibited by influential members of staff. Despite the possible negative effects, information security knowledge sharing should be encouraged because many employees do not have the skills necessary to make security judgements, thus informal learning opportunities can be of benefit within an organisation. Furthermore, formal information security processes and organisational structures increase the amount of informal knowledge sharing that takes place.

2.2 LITERATURE REVIEW ANALYSIS

Existing literature shows that several frameworks for establishing or discussing what constitutes an information security culture have already been proposed. These are predominantly based around models of organisational culture as defined by Schein [61] or Detert et al. [15] and, as alluded to in Section 2.1 by Ruighaver et al. [56], are either too abstract or too granular. Very abstract models contribute to the overall discussion of what constitutes an information security culture but provide little

guidance on how to implement theoretical ideas. Conversely, the finer grained models are beneficial when considering individual behaviours, actions or policies and may prove valuable in defining the why and how of specific policies but are less portable between industries.

Given this critique of proposed frameworks, the assertion that no single model is suitable for defining an information security culture seems reasonable. However, it should surely be possible to develop a model that is sufficiently abstract to be applicable across the full spectrum of organisations whilst also providing suitably concrete guidance which will enable individual organisations to develop an effective security culture.

An analogy may aid in understanding where a model for an information security culture is likely to sit. Consider a house: there is no single blueprint for building a home. Instead, architects design these buildings to meet the needs of the (prospective) owners, knowing that rooms such as a kitchen, communal living areas, bathrooms and bedrooms will be required. If all houses were built from a single blueprint then each one would be identical and unable to meet the different needs of individual home owners. However, there are accepted fundamental requirements for every home which are sufficiently granular to allow them to be easily implemented whilst remaining abstract enough that they can be conceptualised to meet any housing need. A framework for an information security culture ought to be positioned similarly.

Most of the studies reviewed in Section 2.1 highlight the need to consider how human behaviour contributes to security effectiveness. Many also assert that training is required to address undesirable behaviour, with one paper [76] almost implying that no mistakes will ever be made in a security-positive culture. The latter position is very unlikely to ever be achievable. Instead, as another paper [62] suggested, mistakes and errors should be reported so that they can be seized as opportunities to learn and improve, and only prompt disciplinary action in cases of malicious intent. An environment where no mistakes are made can thus be seen as the ideal aiming point to which an organisation draws ever closer with each lesson learned.

2.3 COMMON FRAMEWORK REQUIREMENTS

The ideas and models discussed during the literature review provide the following useful list of common points that should be remembered when attempting to define an information security culture framework. These can be summarised as follows:

1. Human factors are as important as physical, procedural and technical controls.
2. A security culture is a sub-culture of wider organisational and national cultures, and is influenced by these.
3. A security culture is made visible by actions and processes that are determined by knowledge, motivation, commitment and behaviour, which are in turn influenced by underlying beliefs and assumptions.
4. A security culture helps to provide a long-term security strategy within an organisation and should be subject to continuous change based on risk management, feedback and evolving organisational requirements.
5. Leadership should lead by example, exhibit commitment and have both defined responsibilities and upwards managerial accountability.
6. Trust and communication must be bi-directional.
7. Training, education and knowledge sharing are vital to the continuing improvement of security practices.

2.4 SAFETY CULTURE

Safety culture has previously been suggested[1] as a possible foundation from which to develop an information security culture [44]. It is notable that no additional literature has been produced to either take this concept further or dismiss it. These previous suggestions add weight to the validity of the motivation underpinning this thesis and the first step needed in the development of a model based on safety culture is to explore what constitutes a safety culture.

Safety culture focuses on understanding how human behaviour can contribute to organisational level accidents and has been extensively written about by Reason

[1] O'Regan [44] notes this was first suggested by the Information Security Forum in an article published in 2000, but attempts by the author to locate a copy of the original document have been unsuccessful.

[54][52][53][51], a subject matter expert. The following summary provides a concise overview [53].

The overarching aim of safety culture is to maximise safety in relation to organisational accidents, irrespective of leadership or commercial agenda. Acknowledged as hard to achieve, it relies on the ongoing consideration of how safety can be compromised. The right data needs to be captured, analysed and communicated, having first been sourced from incidents, near-misses and regular system health checks. A safety culture is an informed culture which relies on understanding the human contribution in an otherwise technical environment and is comprised of a series of sub-cultures.

Each sub-culture is a fundamental pillar of the higher-level safety culture. A just culture is one in which staff are encouraged to report their own mistakes, and those of others if need be, and to trust that the organisation's leadership will set clear lines between acceptable and unacceptable behaviour, for which sanctions will be imposed. A reporting culture is one which depends on the willingness of employees to report errors and near-misses. Such a culture depends on the underlying attitudes an organisation has regarding blame and punishment. An organisation must be capable and willing to draw not only the correct conclusions from its safety system, but to also implement necessary reforms when the system indicates a need to do so – a learning culture. Finally, organisational training must be provided to give line managers the awareness of when to hand control over to technical experts, and training to the latter to enhance their expertise. This promotes a flexible culture, where operational structures move from hierarchical to ones based on professional skills in times of crisis or high intensity workloads.

Furthermore, a safety culture is something an organisation is rather than what it has. Yet, it is necessary for it to have all the requisite constituent parts, thus what an organisation has. In these terms, what an organisation is, is determined by the sum of the interactions of each of these constituent parts and this is what provides the reward. Such an ideal is something that must be striven for yet is rarely achieved; rather, the main value comes from the act of striving [53].

Although the above explanation of a safety culture is relatively complete, it does not correspond to the final model that will be used for exploring an information security

culture. The final model originates from the MAA and expands on Reason [42]. The next section describes the reason for the development of an expanded model and provides a brief overview of the constituent requirements of the framework by way of a case study. The argument as to why such a model is suitable for comparison with information security will then be outlined.

Before doing so, however, it is worth explaining the Swiss Cheese model [53], which is one way of considering safety and the cause of accidents. Figure 2-1 shows a graphical representation of this model. In an ideal world, each defensive mechanism is viewed as an intact slice of cheese. However, in the real world, each of these defences have holes, either due to active failures or organisational reasons, hence the term Swiss Cheese. An accident occurs when all safeguards, controls and defences are by-passed; a sequence in the holes of each slice of cheese are aligned

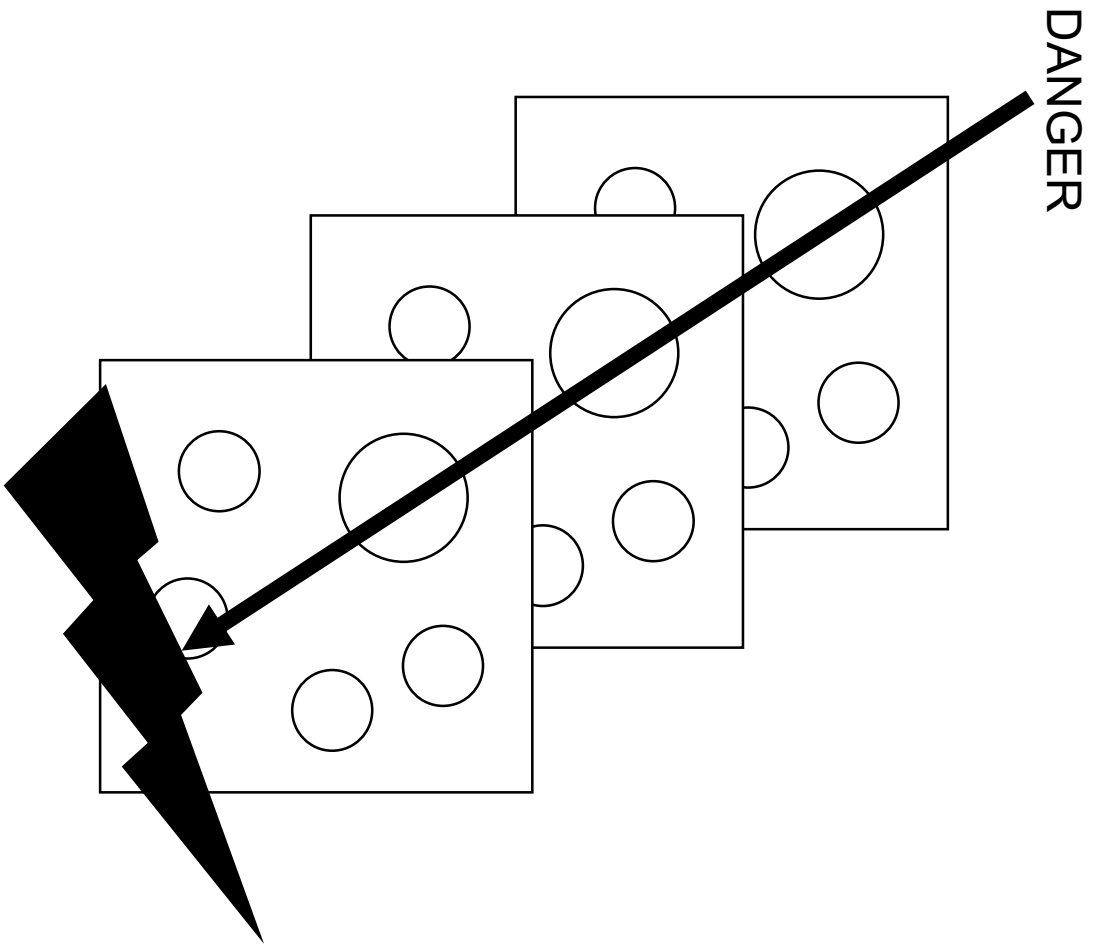

Figure 2-1: Overview of the Swiss Cheese Model [52]

from one end to the other. All it takes for such an event to be prevented is for a single hole to be out of alignment.

A similar view can be taken in information security. Instead of an accident, a security breach occurs when the holes in each slice of cheese are aligned, causing all safeguards, controls and defences to be bypassed. Again, just a single hole being out of alignment can prevent the breach from happening. The practice of information security, then, is about keeping as many holes as possible from becoming aligned. Keeping this idea in mind may be helpful when considering the relevance of the concepts that will be introduced throughout the remainder of this thesis.

2.5 FROM SAFETY TO AIR SAFETY

On 2 September 2006, a Nimrod reconnaissance aircraft of the UK's Royal Air Force (RAF) crashed in Afghanistan, killing all 14 crew members on-board. Initial reports suggested the cause of the crash had been a technical fault with the aircraft, rather than due to any hostile action [4]. Further investigation [5] revealed that the aircraft had exploded in mid-air shortly after conducting air-to-air refuelling, resulting in the biggest single loss of life to UK military personnel for a quarter of a century. A Board of Inquiry convened by the RAF found that old equipment and a lack of fire suppressant systems contributed to the loss, which was caused by a fuel leak; this led to accusations that the MoD had been cost cutting. In May of 2007, a coroner ruled that the aircraft had never been airworthy and in December of that year John Hutton, then Defence Secretary, was served with a writ accusing the MoD "*of negligence, failing to minimise risk and a breach of the right to life*" [6]. It took until March 2009 for the MoD to admit that the aircraft was not airworthy [7].

On 13 December 2007, the UK's Defence Secretary appointed Haddon-Cave QC to conduct an independent review into the Nimrod crash. Specifically, he was to consider the issues surrounding the loss of the aircraft. His report, *The Nimrod Review* [25], published on 28 October 2009, attributed the crash to "*a failure of leadership, culture and priorities*". *The Nimrod Review* noted that most of the lessons to be learned were not new and comparable to other accidents of a similar scale. Among those highlighted in the review are the King's Cross fire, the Space Shuttles Columbia and Challenger, the Herald of the Free Enterprise and the Marchioness

Disaster. Key findings from *The Nimrod Review* are summarised as: "*a failure to adhere to basic Principles…a Military Airworthiness System that is not fit for purpose…a Safety Case regime which is ineffective and wasteful* [and] *a Safety Culture that has allowed 'business' to eclipse Airworthiness*" [25]. Four recommendations were made to address the key findings:

1. Adherence to four new principles – leadership, independence, simplicity and people [25].
2. Introduction of a new airworthiness regime which promotes new attitudes and behaviours, is relevant, effective, and understandable, and which facilitates a new safety culture [25].
3. Define risk cases, which are specific, relevant and proportionate [25].
4. Introduce a new safety culture comprising five key sub-cultures – just, reporting, learning, flexible and questioning [25].

In response to *The Nimrod Review*, the MoD established the MAA in 2010 [55]. The MAA is an independent and autonomous body within the MoD with responsibility for developing and enforcing air safety regulations, promoting an engaged air safety culture and providing an independent assurance process [20].

Given that there were no new lessons to be learned from this accident, the comments and summary of the review seem fair. Considering that the Nimrod crash and security breaches such as those highlighted in Section 1 were comparable to previous events, would it be fair to suggest that Haddon-Cave's key findings could also be applied to the information security approach and priority of many organizations?

A 2017 report [8] suggests that Chief Information Security Officers "*are too focused on the technological and operational dimensions of cybersecurity, at the expense of business impact and risk management*". A key finding from another report [49] is that information security is particularly strong in organisations where the board of directors is engaged in such issues. Findings like these suggest that for many companies where information security is not high on the board's agenda, security is not a top priority, is poorly understood and poorly implemented. So, whilst some may disagree, the author believes it is fair to suggest that conclusions like those of The Nimrod Review can be applied to information security practices. It thus follows that a

similar overhaul is required and that organisations need to think about information security in a new context, which will be termed an engaged information security culture.

2.6 FROM AIR SAFETY TO INFORMATION SECURITY

Having established in Section 2.5 that information security ought to be considered in a new context, it is now necessary to illustrate why safety culture provides a suitable foundation for doing so. By drawing comparisons between air safety and information security, their management systems and cultural definitions, an initial model for an engaged information security culture is proposed.

A common definition for information security is the "*preservation of confidentiality, integrity and availability of information*" [11].

The MAA assert that:

> "*Military Air Safety is 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*" [20].

Initially, these definitions appear considerably different. The definition of air safety is written from a prevention perspective whilst information security's is from a retention point of view. Also, the definition of information security makes no mention about how long confidentiality, integrity or availability should be preserved. A reasonable assumption is that these properties should be for the lifetime of a system or service – a comparable view is that of cover time in cryptography [39].

In contrast to air safety, the definition of information security does not account for hostile activity. It is fair to expect military aircraft to be exposed to such events, but does a cyber-attack warrant a similar categorisation? The General Data Protection Regulation (GDPR), in addition to requirements concerning the confidentiality, integrity and availability of processing systems and services, introduces the need for resilience [26]. This formalises a requirement for information security practices to be

able to cope with and recover from attacks. In other words, how hostilities are handled.

Considering this, a revised definition of information security, which draws from the MAA [20] definition of air safety as well as the GDPR [26] as grounds for the inclusion of resilience, is:

Information security is the state of freedom from unacceptable risk of loss of information confidentiality, integrity, or availability throughout the life cycle of a system or service. It extends across all organisational areas and addresses resilience to an attack.

Having shown that information security and air safety can be considered in comparable terms, what can be said of the systems used to manage each of these? The International Civil Aviation Organisation (ICAO) defines a Safety Management System (SMS) as:

> "*a system to assure the safe operation of aircraft through effective management of safety risk. This system is designed to continuously improve safety by identifying hazards, collecting and analysing data and continuously assessing safety risks. The SMS seeks to proactively contain or mitigate risks before they result in aviation accidents and incidents. It is a system that is commensurate with the organization's regulatory obligations and safety goals" [29].*

The MAA [42] definition of an Air Safety Management System (ASMS) expands on the ICAO definition, to include "*the entirety of all documented and undocumented structures, processes, procedures, tools and methodologies, enabled and underpinned by the prevailing Air Safety Culture, that exist to manage Air Safety*".

An ASMS is like an Information Security Management System (ISMS), which the ISO/IEC state:

> "*consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing,*

maintaining and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks" [11].

The key themes common to both an ASMS and an ISMS can be summarised thus: the management of risk to ensure business objectives are met using a structured approach, whilst continuously striving to improve the effectiveness of the risk management process. Unlike the MAA definition, the ISO/IEC definition does not make any specific reference to an organisation's cultural approach to information security management. Eight principles that are fundamental for an ISMS to be implemented successfully, such as the requirement for management and stakeholder buy-in and improving societal values, are highlighted in the ISO/IEC 27000 series of standards [10][11]. Combined, these principles could be considered as underpinning cultural aspects necessary to ensure the effective management of information security.

This prevailing air safety culture, which is essential to the effective management of air safety, is defined as an engaged air safety culture. Such a culture:

"*is that set of enduring values and attitudes, regarding Air Safety 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 safety; is willing and able to adapt when facing safety issues; is willing to communicate safety issues; and continually evaluates safety related behaviour*" [42].

The model for an engaged air safety culture developed by the MAA has values and behaviours components and underpinning components, as shown in Figure 2-2 [42]. This model builds on the work of Reason [53], who has been established as an authority on the subject in Section 2.4. In addition, it incorporates the recommendations made by Haddon-Cave [25] from Section 2.5.

It follows that without an effective information security culture, an ISMS will be unlikely to achieve its objectives. Accordingly, and due to the intellectual rigour that

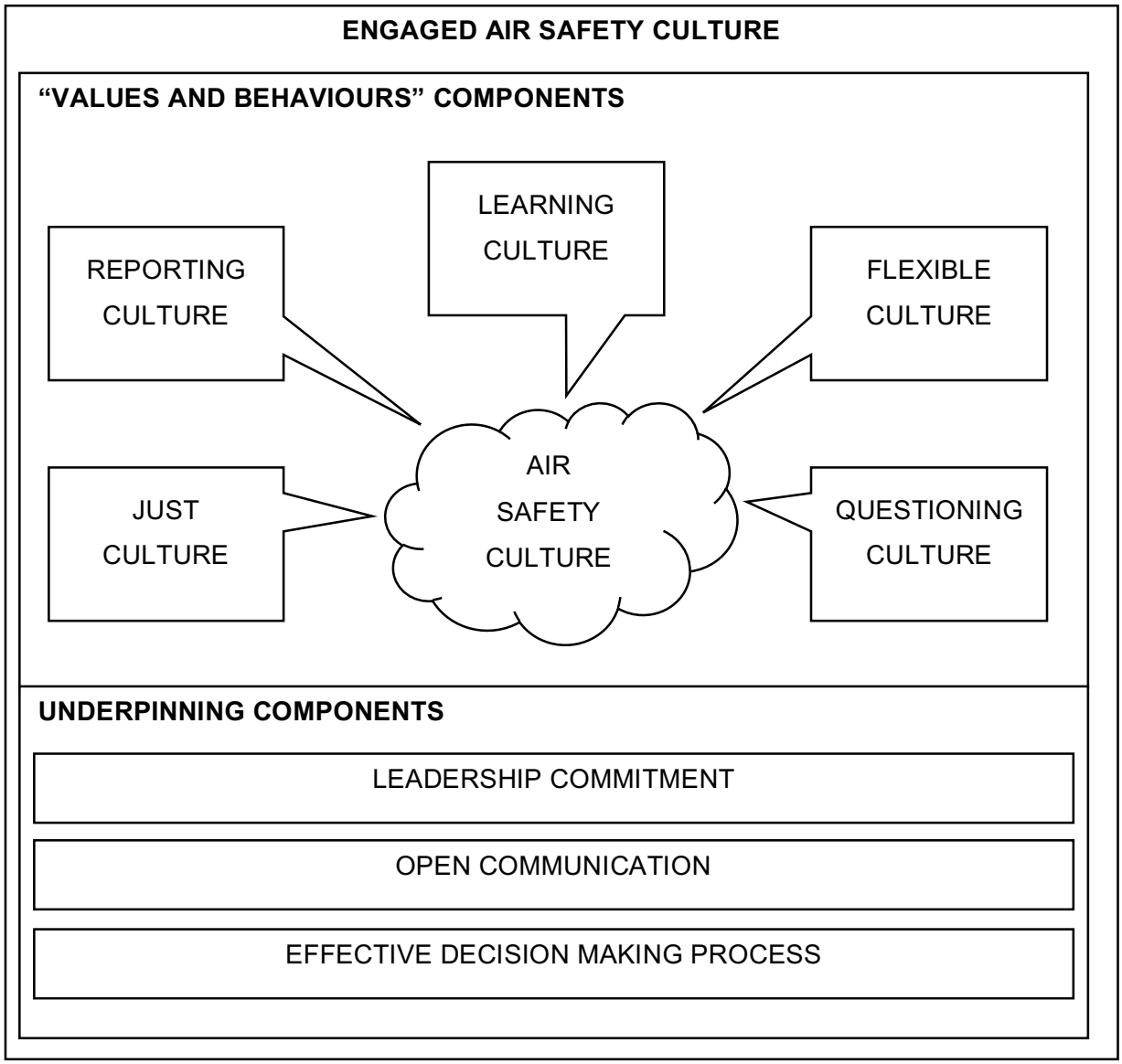

Figure 2-2: Model for an Engaged Air Safety Culture [41]

has gone in to its development, the MAA model for an engaged air safety culture is a good framework to explore a model for an engaged information security culture. Borrowing from the MAA [42], to be read in conjunction with the earlier definition of information security:

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.

In the coming sections, each of the values and behaviours components will be unpacked in turn, followed by the underpinning components. A summary of the final model then follows.

It is worth noting that the MAA definitions in the following sections often refer to an Air Safety Incident Management System (ASIMS), which forms part of a wider Defence Aviation Error Management System that is used for all aspects of occurrence reporting, recording, monitoring and investigation [42]. For the purposes of this thesis, it is assumed that a comparable system is available for carrying out these functions in relation to information security. Such a system will be referred to as an Information Security Incident Management System (ISIMS).

SECTION 3 JUST CULTURE

3.1 WHAT IS A JUST CULTURE?

The following summarises Reason [53], who's credentials are established in Section 2.4. A just culture is likely unattainable, but an organisation where employees believe justice will be carried out is achievable. Punishing all errors irrespective of their origin is unacceptable, as also is complete immunity from any form of discipline. Most errors result from organisational failings rather than through recklessness or negligence, although these are not impossibilities. A just culture, then, must differentiate between truly bad behaviour where punishment is warranted and that where assigning blame is inappropriate and not useful.

To establish which category a certain behaviour falls into, it is necessary to understand how behaviours form. Decisions are taken based on feedback from experience and actions perceived as necessary to attain desired outcomes. Experience is derived from past outcomes, training and actions guided by procedures (collective experience and wisdom). The risks associated with conducting an activity should therefore reduce as the experience of those making decisions increases.

These decisions, or behaviours, can either be successful or unsuccessful, correct or incorrect. A successful behaviour, however, is not necessarily a result of a correct behaviour – a desired outcome may be achieved through incorrect behaviour. Conversely, it is possible for correct behaviours to be unsuccessful. Unjustifiable risk taken deliberately is reckless behaviour. Taking an action without being aware of the risks, where a reasonable person with equivalent experience would have been aware and so avoid taking the action, is negligent behaviour.

Before deciding whether a behaviour falls into any of these categories, it is important to determine if the behaviour taken by a person would also be taken by their peers given the same set of circumstances. If yes, then no blame should be apportioned because the failure is likely to be organisational, thus, whilst undesirable it is not unacceptable behaviour.

Furthermore, the intention behind such behaviour is also important to consider prior to ascribing it as reckless or negligent. Unintended actions are in the category of lapses whilst unintended consequences are either mistakes or violations. It is necessary to ascertain what was being done at the time of a lapse before culpability can be determined. For violations, if committed knowingly, culpability should be higher due to an awareness of increasing risk. However, this still does not mean any undesirable consequences were deliberate and must be accounted for during investigations, along with consideration of any mitigating factors.

Most violations are not carried out with the intent to provoke unwanted outcomes, i.e. they are non-malevolent. If this were not the case, it would be sabotage. Thus, it is also necessary to consider during investigations the quality of training and procedures. If either of these are not at the required standard, or if a pattern of organisational shortcuts has emerged, incorrect actions or consequences again reflect organisational failings. As before, whilst undesirable it is not unacceptable behaviour and blame should not be apportioned.

Determining whether to assign blame must be exercised with extreme care and judgement, and only following a fair and impartial investigation. Over 90% of unsafe acts fall into the category of blamelessness. Behaviours falling within this band should be viewed as acceptable. For the remaining small percentage of offences, punishment can be worthwhile and encourages the remainder of employees to see the organisational culture as just, especially if habitual rule-breakers are punished. Provided such punishment is viewed by employees as fair then it will improve morale and help reinforce the lines between what is acceptable and unacceptable behaviour.

For the purposes of air safety, the MAA assert that "*all personnel must understand that honest errors can be made and a Just Culture 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*" [42]. Failure to implement such a culture is likely to have a negative impact within an organisation, with people's morale, commitment, job satisfaction and willingness to go the extra mile all being reduced [14].

Given the difficulties inherent in fairly determining culpability, it is clear to see why Reason suggests a just culture is likely to be unattainable. However, striving for one is of paramount importance.

The following summary of a case study by Dekker [14] serves to highlight the difficulties involved in determining culpability and delivering justice. It is purposefully lengthy to ensure sufficient detail is presented and to show how a situation as viewed after an event, with the luxury of hindsight, can be interpreted very different from how it is seen as circumstances unfold.

3.2 SAFETY CASE STUDY

A Boeing 747 on approach to London Heathrow airport had to conduct a second approach due to being misaligned with the runway in heavy fog on 21 November 1989. When the pilot initiated the procedure to abort the first approach the plane was outside of the airports perimeter and about 75 feet from the ground. Narrowly missing a collision with a hotel, it set off the buildings fire sprinklers and the alarms of nearby cars. Two and a half years later, in a case which divided a jury and the aviation industry, the experienced captain with 15,000 flying hours was found criminally guilty of negligence.

Prior to this incident, during a layover in the Maldives, the crew's co-pilot and flight engineer contracted gastroenteritis. On the advice of an airline approved doctor the crew saw a Mauritian doctor, who was soon to be added to the company's list of approved physicians. This doctor suggested the flight engineer take some of the tranquilizers and painkillers prescribed to his wife, who was also on the trip and ill. It is suggested that the doctor would have been reluctant to prevent the crew from flying, as the company would have taken a dim view and be unlikely to employ him in future. En-route to London the co-pilot took some of these pills and had to leave the cockpit, with the captain left alone to fly the plane in the dark for five hours.

Over Germany, the crew were advised of heavy fog at Heathrow, which would require the plane to effectively be landed blind. The minimum weather limits for such an approach mean that the plane's wheels may have poked out of the fog as the aircraft flared during landing but the cockpit would still be in the clouds. These approaches are flown by the autopilot, leaving the crew to monitor progress.

However, the captain, despite his considerable experience, had never flown to these minimums – like most pilots. The co-pilot wasn't even approved to fly such an approach.

As was standard practice, the captain contacted the company and asked for a dispensation allowing the co-pilot to operate in these conditions. As usual, it was granted without question and the co-pilot accepted, although would not have minded diverting to somewhere with better weather. This, however, presented a conundrum for the sick co-pilot. What would the airline say if either the captain had not made the request as standard or he had not accepted it? If a diversion was made due to him being too sick to carry out the procedure, why was he onboard and where had the medicines come from?

As one observer put it, in one ear the airline says never compromise safety or procedures, yet in the other, don't cost us money, don't find reasons not to get passengers to their destination. A conflict of interests if ever there was one.

In a holding pattern over London with only two minutes of holding fuel remaining, air traffic control cleared the aircraft to begin an approach. However, the wind direction had changed and the crew would have to make the approach to a different, unplanned and much closer runway. They hurriedly revised their mental picture of the landing process and updated their charts. The approach controller turned the plane onto the localizer (a radio signal forming part of the instrument landing system that the autopilot uses) at 10 miles rather than the usual 12 miles. Amid various other distractions on the approach, including delayed landing clearance due to another plane being too close and still on the runway, the autopilot struggled to obtain and maintain the required signals from the landing aid. The system installed in the aircraft had been retrofitted, having not been designed for a 747, and needed to be carefully managed.

Technically flying illegally due to the imperfectly functioning autopilot, hindsight says the captain should have abandoned the approach and repositioned to try again. Others have pointed out that he would have been concerned with needlessly costing the airline tens of thousands of pounds by doing so, the limited fuel and the condition

of the co-pilot[2]. It is not unknown for the autopilot to settle down eventually nor for the aircraft to break clear of cloud at a less stringent limit, enabling the last part of the approach and landing to be flown visually. Had this been the case, there would have been no incident in the first place. However, that wasn't to be and the captain eventually elected to fly away and try again, this time uneventfully.

That same evening, the crew was suspended. An investigation was launched and in a report both the co-pilot and flight engineer were chided. The captain was demoted, prosecuted and later resigned. The airline stopped granting dispensations in poor weather a short while later, yet the person who authorised this decision was not put on trial, and neither was the controller who turned the plane onto its landing approach too close to the plane ahead. The 747's autopilot was never checked to see if it functioned correctly and four pages of the maintenance log remain missing (their content is unknown as is whether they could have shed valuable light into the system's functionality). The airline's procedures allowed the captain to make an illegal approach by granting dispensations to unqualified pilots. Had that not been so, the captain would have diverted and yet neither the company nor regulator faced prosecution. The defence showed that the entire landing procedures, as required by regulation, take seven minutes to complete but this approach only took four, so it would have been impossible to follow all the rules.

The trial revolved around technical and legal points. The captain, accused of negligence and breaking the company's medical procedures, was never asked to testify. Yet the jurors, who sometimes napped and although split in their decision, still found him guilty.

3.3 ANALYSIS

As the preceding case study shows, the combined decisions and actions of multiple people resulted in an outcome that some viewed as recklessness and others as an organisational failing. The difficulties discussed in Section 3.1 when determining culpability and whether to apportion blame are clearly highlighted in this example, yet being able to do so is essential to achieving a just culture. The following

[2] The observer's comments about a conflict of interests, above, could equally apply here.

observations, whilst focusing on information security, are equally applicable to any industry.

Similarly to what has been seen in this example, multiple complex technological components all interact in today's information and operational technology systems. They are not necessarily designed for the function in which they are being used, are operated by different groups of people, and may be legacy systems. This latter point is especially relevant when considering industrial control systems and enterprise environments, where newer technologies are retrofitted or 'bolted on' to achieve greater functionality [37].

All security investigations need to bear in mind that whilst a security incident or breach may become manifest as a consequence of a lapse or violation by an individual, in most cases there will have been many other factors within the organisation that contributed to it. Therefore, apportioning blame, scapegoating and punishing an individual or group should be avoided. In many cases, except where it is clear to all concerned, doing so is likely to cause division, especially if the investigation appears to be unfair or not impartial. Furthermore, valuable lessons and opportunities for improving organisational processes are lost. Dekker [14] notes this is especially true if one or more people are being prosecuted as a consequence.

Accountability for actions can still be maintained without blame and punishment. Resignation should not be considered a form of accountability, and is backwards looking; it, along with dismissal and other forms of punishment, do not facilitate learning from these events [14]. One solution for holding to account employees who have had a lapse or committed a violation would be to include them in the process of learning from the incident.

From the explanation of a just culture in Section 3.1, including employees in the learning process can help to reinforce in them a view of fairness and that human factors are taken seriously. When staff perceive an organisation to be fair, trust is fostered. Inclusion in learning from an incident also positively impacts on the common requirements of an information security culture identified in Section 2.3. Learning develops knowledge, which should positively alter the underlying beliefs and assumptions of staff. In turn, this would influence motivation, commitment and behaviour, and eventually actions and processes.

These activities serve to enhance experience, which is shown in Section 3.1 as being vital to enabling staff to make decisions with minimal risk. Since over 90% of incidents have no beneficial grounds for ascribing culpability, a just culture when correctly created and operated provides a significant opportunity for reducing risk.

3.4 SECURITY CASE STUDY

The evidence from the following account [58] highlights an incident that appears to have occurred outside of a just culture. An exemplary contractor was fired after losing an unencrypted USB drive containing 6,000 medical records, after being unable to transfer the files in the usual manner. Transporting data by USB was against company policy. The CEO noted that the employee was likely unaware of being in breach of company policy, but that it was a mistake that should not have occurred.

From the information available in the article, this seems to be an organisational failing rather than deliberate malicious behaviour. Given that the CEO admits the contractor was likely unaware of the policy they were in breach of, the best solution would have been to review why employees were unaware of policies, make them more visible and develop procedures for use when the normal process fails. Other staff may even have used a USB to transfer data when the usual mechanism was unavailable. Accordingly, they may well feel that firing the contractor was unfair, leading to fractions within the company. Instead of holding the employee to account and including them in the review and subsequent learning process, the organisation in question likely wasted a valuable opportunity to meaningfully improve their security and foster a reputation of fairness among its staff.

3.5 SUMMARY

The ability of a just culture to reduce risk is predicated on acknowledging that people make mistakes, that mistakes need to be dealt with fairly, and that justice needs to be preserved. Such attributes are applicable to a wide number of industries and could be considered generic. It follows that a just culture is necessary within an engaged information security culture. For this model, the MAA [42] definition is used verbatim:

All personnel must understand that honest errors can be made and a just culture 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.

Finally, it is important to note that a just culture in isolation cannot provide the necessary learning to ultimately result in reduced risk. This can only be achieved after obtaining a thorough understanding of an incident and related events. For an organisation to acquire this information, its employees need to feel confident to provide it and have a means of doing so. A just culture is therefore instrumental in the creation of a reporting culture.

SECTION 4 REPORTING CULTURE

4.1 WHAT IS A REPORTING CULTURE?

The MAA state "*open and honest reporting of safety concerns by stakeholders at all levels is essential, to understand and manage the potential causes of future accidents. The understanding and exploitation of a Just Culture and ASIMS are vital for a healthy reporting culture*" [42]. A reporting culture, therefore, is a culture which encourages employees to provide information that can be used to gain insight into how problems might unfold in the future,

The following is a summary of Reason [53]. It is hard to convince people to report incidents and errors. People can be easily deterred from doing so if they do not consider it a worthwhile activity, anticipate punishment, do not believe they have made an error or are reluctant to admit to having done so. Yet, many very effective reporting programmes exist, such as those employed by NASA and British Airways, and can be used to provide indications of best practice approaches for implementing and achieving a reporting culture. Although they are predominantly aviation focused, schemes in other industries such as healthcare have been successfully modelled on them.

There are five main factors that must be addressed when developing a reporting culture. The first three address the issue of trust in the reporting system; those remaining provide motivation to submit reports:

1. Protection from disciplinary actions where practicable.
2. Anonymity or confidentiality.
3. Separation of report collection and analysis departments from disciplinary bodies.
4. Provision of fast, accessible, useful and clear feedback.
5. Simplicity of reporting.

Reporting systems should provide feedback on local and organisational factors rather than being used to ascribe blame. Staff should be protected from disciplinary action based on the contents of a report, although there will be limits to this, such as if breaking the law. Section 3 discusses punishment and justice in general.

Reports need not be anonymous, but a separate confidential reporting system helps provide extra detail that can be informative; these must be de-identified to prevent their purpose being undermined. Complete anonymity is disadvantageous since it prevents follow-up questions being posed by investigators. It may also lead to the perception that reports have been sent by a dissatisfied employee, and result in the report being ignored. Further, small organisations may find it impossible to ensure anonymity in practice. Considering this, reporters details should be collected as part of a report, with de-identification occurring in the report handling process. It is important to ensure this happens, and that the procedure for doing so is known by all potential reporters.

Reporting systems should be separated from regulating bodies and employing organisations. If the latter is not achievable, it should be entirely independent of line management. This helps to ensure confidentiality is maintained and remove fear of reprimands by supervisors.

A lack of useful feedback from submitted reports is detrimental to the quality and frequency of incident and error reporting. Where a pattern of hazardous events is noticed, an investigation should be initiated and an alert issued to enable rectification. Data should be made available, and searchable, within the organisation, to researchers, academics and interested parties from further afield. Regular newsletters help describe safety issues and improvements, being both informative to staff and a form of congratulation for their ongoing contribution to safety. They could also include details on trends, risks and the status of investigations.

Reporting ease is vital to ensuring that reports are submitted by staff. Apart from the absence of privacy guarantees, a long, complex, or negative focus to a form will deter people from completing it. Although simple multiple choice questions are easier to analyse, they can limit the value of information obtained from reports. Open questions on a range of potential factors elicit a better picture of the situation and perceived contributing factors, but requires a higher analytical workload. Despite this, it should be favoured, and ultimately will require an element of trial and error prior to achieving an optimal reporting form that is both easy to complete and enables effective analysis within the constraints of the available resources.

Irrespective of the approach taken, questions should be categorised in a manner that facilitates employees' answers being used to establish what happened and why. Gaining a picture of behaviours and outcomes is relatively straightforward; determining the reasons takes more effort. Factors such as employee or team behaviour, organisational, environmental and personal influences help to establish causal links. Understanding these links is necessary before being able to answer why something happened.

Commentary by Syed [71] explains that a reporting culture provides a means of feedback, although this will only be forthcoming if staff trust the system and are sufficiently motivated to use it. The reports submitted need not focus solely on accidents. In aviation, errors not leading to an accident, such as narrowly missing another aircraft or flying at an incorrect altitude are rich learning opportunities. When such errors are committed, pilots are required to submit a report which is anonymised prior to publication, enabling trends and possible problems to be identified and dealt with before a more serious incident occurs. The MAA suggest [42] a ratio of at least ten observation reports for every one realised accident or incident is preferable to support a predictive rather than a reactive approach to risk management.

The following two case studies are taken from aviation and healthcare respectively. They are useful for highlighting the benefits of a reporting culture and the potential consequences of not implementing one.

4.2 SAFETY CASE STUDY

The first case study summarises an example from Syed [71], and succinctly shows why a reporting culture is beneficial. In 2005, a series of reports were submitted in a very short space of time by pilots mistaking lights on top of a newly constructed mural for the runway lights of a Kentucky airport, causing them to approach the airfield too low. Aviation safety experts responded quickly, notifying scheduled flights of the distraction and engaging with the local authority to remove the mural, thus preventing an accident before it could happen.

Conversely, Dekker [14] provides an example of a medical case in which an anaesthesiologist administered a paralyzing agent to a patient at the beginning of

surgery. As the surgery was ending, he reached into his draw for the reversal agent. Both vials were side by side, with yellow labels and yellow caps. The incorrect agent was selected and administered to the patient. In this instance, there was no bad outcome from the situation. Yet when discussing the incident with colleagues, it became evident they were all aware of the potential for confusion but none had raised it as a hazard.

It is not known whether there was any mechanism for the anaesthesiologists to provide feedback or if non-reporting resulted from fear of reprisal. The scenario raises the question of whether it is possible to prevent people from making mistakes by instilling in them a fear of the consequences of doing so? Or would prevention be better achieved by inviting people to report hazards and errors, thereby creating an opportunity for rectification?

4.3 ANALYSIS

These case studies help to highlight some of the benefits of a reporting culture as well as drawbacks of not having one. The first shows that by collating many similar reports filed in quick succession, it was possible to take swift action to prevent a problem becoming a major accident. Protection from disciplinary action and either their anonymity in, or the confidentiality of, reports meant that flight crews were not afraid to file a report, even though they had been too low on approach (a lapse or violation, depending on your point of view). In stark contrast, the second scenario illustrates just how difficult it is to obtain meaningful feedback that could significantly improve safety if a reporting system is not in use. It should be noted that identifying actions to address issues raised in a report are considered as elements of a learning culture, which is the focus of Section 5.

An information security culture, then, cannot be established without a mechanism for employees to provide these valuable incident and error reports. However, such a system alone is insufficient and must be built on the foundation of a just culture, guaranteeing reporter confidentiality and immunity from disciplinary action based on the content of their report. In the situation with the anaesthetists it may be that such a system did exist but these guarantees were not in place, causing anxiety to prevent them from reporting problems.

Guarantees of reporter confidentiality, which is preferable to anonymity, although anonymous reports can be of benefit, enables employees to be asked follow-up questions if needed but ensures their details are removed from official documents [53]. A similar confidentiality approach could be taken for the circumstances leading to an incident. A few comments from personal observation may help clarify this point.

Military aviation incident reports need to contain details about the circumstances of an occurrence. However, when operating in some sensitive environments, the specific details cannot be made generally available due to the security classification of the event. In such situations, reports are still acted upon in the normal way, but in a manner that observes the security requirements. Once submitted, the original report is retained but a copy with the sensitive material redacted is published to a more generally accessible system. Such reports retain sufficient detail as to be useful to any investigators (who may additionally be granted access to the original) or readers without providing any secret information.

The point here is that a similar approach to reporting could be taken within organisations. Sensitive intellectual property, business processes and systems configurations can be prevented from being made available to a wider audience than necessary, whilst at the same time ensuring that reports contain sufficient detail as to not make them meaningless.

Fast feedback in the first case study enabled the lights to be removed. Based on Reasons [53] comments, this would have encouraged pilots of the validity and usefulness of the reporting system, demonstrated the benefit of reporting, and acted as a reward because safety was enhanced in this instance. Similarly, feedback from information security reports should have a visible impact to encourage staff to engage.

Many airlines collect data in real-time to enable areas of concern to be identified, which the Royal Aeronautical Society [36] have said dramatically improves safety. Therefore, collecting security data in real-time, or as near to real-time as possible, is likely to have a similar impact. Organisations may already have some form of business event reporting system or Security Incident and Event Monitoring (SIEM) systems in place, which could be used to generate automatic reports [69]; simple collation of these and providing feedback to staff may prove to be a useful first step

in this direction. Additionally, some organisations already report details of breaches or incidents to third party companies [22][78][3], which are used to compile trends and highlight some general lessons.

Ultimately, however, dedicated information security reporting systems should eventually be implemented to enable organisations to compile, analyse and learn how to improve their own processes and reduce risk. These would ideally be similar to ASIMS, used by the MoD, or those of NASA and British Airways mentioned in Section 4.1. Such systems need to be designed for simplicity and ease of use, yet capable of capturing relevant information which provides useful feedback to security management teams, who should be separate from any disciplinary body. Not only can this information be used to provide feedback to the wider organisation but it can help with continuous monitoring and review requirements of an ISMS [10].

Staff should be encouraged to report not only security breaches and incidents but also events and any of their own or others' actions that could have resulted in these occurring. Doing so contributes to the common requirements established in Section 2.3. Patterns and trends can be identified, reducing risk and enabling long-term strategy to be devised and evolved. Deficiencies in training, education and knowledge can be exposed and action taken to rectify the shortfall. Eventually managerial trust in employees will grow, and vice versa, improving bi-directional communication and resulting in freer flow of information. Business leaders can use such a system to demonstrate their commitment to information security to employees, whilst at the same time using it to aid accountability among their managers. Collectively, these will aid in transforming underlying beliefs and attitudes, positively impacting upon employee motivation, knowledge and behaviour. In turn, the visible display of security knowledge and practices within the organisation will ultimately be of a higher quality. Most of these benefits are dependent on how reports are acted upon.

4.4 SECURITY CASE STUDY

PhishTank [46] is a free platform for people to register websites and IP addresses suspected of phishing related activity. Suspected sites are voted on by the

[3] These are just a very small subset of the available third-party information security breach and incident reports.

community, and when sufficient votes have been received a suspected site is upgraded to a confirmed phishing source. The information reported is publicly available, and is used by companies such as Yahoo Mail, McAfee and Kaspersky Lab [47].

Although a relatively simple example, it illustrates how reporting can be widely used to help prevent future occurrences. Through collaborative reporting, patterns and trends in phishing can be analysed and the resulting information used to implement or improve safeguards against phishing attacks. Such information can also be beneficial during information security training sessions to educate staff about phishing sites. Perhaps most striking is the example PhishTank provides for producing reports proactively, rather than reactively, in the wake of an incident.

4.5 SUMMARY

Open reporting opens the doorway to implementing changes, and as one commentator put it when referring to healthcare, "*with open reporting and honest evaluation, these errors could be spotted and reforms put in place to stop them happening again, as happens in aviation. But, all too often, they aren't*" [71]. As has been shown, the comments are equally applicable to information security.

The key point to note is that both a just culture and effective use of a report management system (the assumed ISIMS), which staff are encouraged to utilise, are vital to creating and maintaining a reporting culture. With some modifications to reflect information security, the MAA [42] definition of a reporting culture provides a suitable definition for inclusion within an engaged information security 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 security breaches. The understanding and exploitation of a just culture and ISIMS are vital for a healthy reporting culture.

A reporting culture, however, is redundant without any means to learn from the reports it generates. As such, the next chapter will consider the applicability of a learning culture.

SECTION 5 LEARNING CULTURE

5.1 WHAT IS A LEARNING CULTURE?

As described by Reason [53], a learning culture is built on the foundations of observation, reflection, creation and action. Of these, the first three foundations are straightforward. However, action can be considerably difficult, yet by not implementing reforms highlighted by a safety system the lifespan of an organisation can be cut drastically short. It is, therefore, important that organisations use their safety systems to identify reforms and be willing and capable of implementing them.

As explained by Syed [71], aviation has an abundance of information on failure. After an accident, independent and impartial investigators are granted unrestricted access to the wreckage and any other evidence. Cooperation and full disclosure is encouraged because any evidence compiled in the production of their report is inadmissible in court. The final report is free and public, airlines are obliged to implement any recommendations made, and everybody can learn from the mistakes rather than just a small subset of individuals or organisations.

This values and behaviours component is about making improvements to help reduce the likelihood of future incidents, and thus risk. The MAA sums it up by saying "*learning followed by communication is a central part of an engaged air safety 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 ASIMS*" [42].

Two case studies, one from aviation, one from healthcare, are used to provide examples of a learning culture's benefits. The latter example is also useful for highlighting and addressing some concerns.

5.2 SAFETY CASE STUDY

This first case study originates from Syed [71] and the following summary helps to show how a learning culture not only assists in the identification of the root cause of an accident, but also provides a means for correlating many similar events. This

helps to ascertain and address the underlying causes, which may not be obvious or verifiable when an event is only considered in isolation.

On 28 December 1978, United Airlines Flight 173 was en-route to Oregon from New York. Once the aeroplane had been given clearance to descend into Oregon, the captain conducted the procedure to lower the landing gear. Indications were that the landing gear had failed to engage correctly and the captain requested extra time to troubleshoot the problem. The crew attempted to determine the source of the problem for close to an hour, notifying the captain of dwindling fuel supplies.

Eventually, the aircraft ran out of fuel and crashed into a Portland suburb; 10 people out of 181 passengers plus crew lost their lives. Later investigation revealed that the landing gear had in fact engaged correctly and the airplane could have been landed. During an interview, the captain said that the fuel had depleted too quickly and suggested a fuel leak as the cause. However, his crew had informed him of the reducing fuel levels, but the pilot had been so focused on diagnosing the landing gear problem that he had lost track of time.

A year earlier, in similar circumstances, another aircraft crashed en-route to San Diego killing all on board. A few years prior to this, again in similar circumstances, a plane bound for Miami crashed in the Florida Everglades killing 101 people. Investigators noticed that the underlying cause in each case was a loss in the perception of time.

Investigators looking into the crash of Flight 173 recognised this correlation for the first time and in June 1979 published their findings, along with a recommendation that all airline crews be taught methods of Crew Resource Management. Considered to be a landmark event, after a succession of tragic incidents and rigorous investigation to identify what went wrong, the rate of crashes declined and thousands of lives have consequently been saved.

Failure is taken seriously in aviation. Any indication that something is not as it ought to be is carefully examined to improve safety in the industry. The value of errors is recognised; thus, they are exposed whenever they occur.

A second example, again a summary of one provided by Syed [71], serves to highlight the necessity of both just and reporting cultures as a foundation for a

learning culture. Syed interviewed Dr Gary S Kaplan, who was appointed the Chief Executive Officer of Virginia Mason Health System (VMHS) in 2002. Already a top hospital in Washington State, by 2013 VMHS was rated one of the top hospitals in the world and that year won awards for patient experience and clinical excellence, as well as being named a top hospital by an influential organisation for the eighth successive year.

Recalling the interview, Syed notes that Kaplan visited the Toyota plant whilst on a visit to Japan. He was so impressed by their cultural approach of being open and honest about mistakes and learning from them that he was determined to implement a similar method at VMHS, hoping to help reduce the thousands of lives lost each year due to medical error. Despite his best intentions, the underlying culture at the hospital meant mistakes were frowned upon and blame was rife, much like elsewhere in healthcare, so staff did not use the new system for fear of recrimination and instead kept details of mistakes to themselves.

When a patient died in 2004 through accidental administration of an incorrect drug, Kaplan’s response provided the catalyst for cultural change. Instead of hiding, he issued a full and honest apology and staff realised that they would not be punished for mistakes unless recklessness was evident. Reports of mistakes were submitted, which according to a US Department of Health report helped to uncover latent errors across the full spectrum of healthcare and led to the introduction of measures to reduce the likelihood of them reoccurring. This helps explain why the hospital has received such accolades, as well as a reduction in liability premiums of 74%.

Syed goes on to note that other hospitals have experienced similar results after adopting a learning culture. Lawsuits against the University of Michigan Health System dropped from 262 in 2001 to 83 in 2007. Malpractice claims against the University of Illinois Medical centre fell by half in two years. Both were because of the introduction of an open reporting policy. However, he also notes that the introduction of policy alone is insufficient; the underlying culture must also be changed for such a policy to be effective.

5.3 ANALYSIS

Recall the example security breaches from Section 1. Now consider that patient deaths associated with preventable harm in the US are estimated at 400,000 per year [30]. Pronovost [48] suggests "*what these numbers say is that every day a 747, two of them, are crashing. Every two months, 9/11 is occurring*". Apart from the loss of life, are the frequencies of preventable deaths and security breaches comparable?

The significant similarity between the frequency of security incidents and preventable loss of life is highlighted by the word preventable. Many incidents could be avoided, but lessons need to be learned and communicated so that others can learn from them too. It is likely that this comparison will be criticised, the reasoning being that information security does not result in loss of life[4]. Whilst that may be true, as has been shown in the case studies it is the principles underlying the learning (or lack of) that largely determines the number of preventable occurrences that take place. There is an increasing convergence of safety critical systems with internet enabled systems [50]. How long will it be before news of hospitals being shut down due to a cyber-attack [24][79] becomes news of security breach related patient deaths? The information security community should not wait for such an event to be a catalyst for a culture change, as was the case at VMHS.

Taking the example of Flight 173, it shows that human factors play a significant role in the outcome of a situation. It is easy to be distracted by one problem and lose focus on the state of the rest of a system. Not only does this show the need to pay attention to others, who may have a better overall situational awareness, when dealing with an incident but also that it is important to have access to reports of similar occurrences when conducting an investigation in the aftermath. The reason for doing so is twofold. Firstly, a less desirable outcome may be averted. Secondly, correlation between different instances of comparable events can lead to significant insights, and in turn to the introduction of reforms based on trends that would not be identifiable if each case was only viewed as a single incident.

[4] This was one of the key objections of many people I spoke with when I first began considering the use of safety culture as a basis for an information security culture.

As highlighted in Section 4, such investigation and analysis requires human intellect and cannot be automated. The acts of collecting incident information, reviewing it and determining mitigating mechanisms to enable learning are relatively simple. Case studies can be produced from such information, yet there are currently few quality examples publicly available, and collective learning within the information security community would benefit from more of these [68]. However, there are some resources available, particularly in relation to Advanced Persistent Threats [17]. It should also be noted that many security recommendations have been made over the years, based on learning lessons from reported incidents; some of these are available for free [77][78].

Evidence of actions taken to implement these recommendations seems to be lacking in many organisations, either through inability or unwillingness. In some cases, failure to make necessary reforms may be through ignorance of a problem and its solution; arguably this would fall into the category of not capable. For example, the TalkTalk data breach referred to in Section 1 resulted from an unpatched vulnerability which the company claimed to be unaware of, even though a patch that would have prevented the breach was available [27]. It has long been known that unpatched systems are susceptible to being hacked [32]. The Mirai botnet infects devices that use default usernames and passwords [18]. Yet, these too have been known to be attack vectors for a considerable time [32].

Whilst there may be many valid business reasons for multiple companies to conduct their own analysis of security incidents and trends, lack of a single source of information can make it extremely difficult to know where to look for it. One way of addressing this would be to have a single, national, potentially government-run, organisation to conduct (or at least collate) all security reports and lessons, and provide the wider community with access to them. Development of a more in-depth suggestion and the business plan for such an endeavour, however, is beyond the scope of this thesis.

When it comes to implementing reforms, it may be much harder to oblige companies to do so than in aviation or other safety critical industries. When done properly, determining security controls based on an effective risk management programme can provide adequate security. Even so, that does not guarantee organisations will

put in place measures which they really ought. Considering the means to do this is again an area beyond the scope of the thesis, but one national legislation could be used to enforce action being taken.

Such an approach would likely be unpopular, particularly in companies where ethics or risk are given less consideration than the desire to make as much profit as possible. However, legislation such as the GDPR does seek to hold organisations accountable to the level of risk they are taking [28], and it could be argued that providing a single repository for obtaining information security lessons from the wider community gives companies less excuse when a breach does occur.

Along with the unpopularity of the above suggestion, some businesses are also likely to object to implementing a learning culture because of litigation or reputational reasons stemming from the need to report security incidents [31][41][60]. Section 4.3 provides a suggestion about report confidentiality that could be used to counter such fears. However, based on the observations made by the various hospitals mentioned in the second case study, these arguments against open reporting and learning initiatives seem to be based solely on pre-conceived ideas. From these findings, it is reasonable to assume that organisations who disclose security incidents, carry out thorough investigations, learn lessons and implement reforms are similarly likely to experience a reduction in litigation and an increase in reputation, due to reduced incident rates.

Purely introducing more policies based on identified lessons will not bring about these changes. Instead, the underlying culture must be changed to be conducive to reporting and investigating incidents, learning the necessary lessons and implementing appropriate changes as a result.

5.4 SECURITY CASE STUDY

In April 2017, LastPass [59] posted a blog entry regarding a bug affecting Google Authenticator when used in conjunction with their software. The problem was reported to the company by a security researcher. LastPass subsequently worked with the researcher to learn about the bug and develop a solution. This follows a software problem discovered in March 2017 [67]. In June 2015 [66] the company's servers were hacked into. On each occasion, LastPass made details of the incidents

available publicly and provided information about how they were responding, which was often in collaboration with third-parties.

This brief example highlights the benefits of being open to learning about security problems and working collaboratively in response to those lessons. Furthermore, it shows that making the details of breaches public is beneficial and likely helped to reassure the company's customers, although some no doubt found the news unwelcome.

5.5 SUMMARY

A learning culture addresses many of the points raised in Section 2.3. It will help to identify human factors that lead or contribute to security incidents and provide an effective means of identifying measures to help change underlying beliefs and assumptions. By determining areas where additional training and education may be needed, subsequent improvements in knowledge and employee behaviour lead to improved security actions and processes. It provides a means of long-term strategic thinking and commitment to information security that facilitates increased security by better risk management and feedback whilst evolving with organisational changes. Linked closely to a reporting culture, it helps foster trust that reports will be acted upon without prejudice, a requirement of the underlying just culture, and is evidence of employee and managerial commitment to bi-directional communication.

For the purposes of an engaged information security culture, a modified version of the MAA [42] definition of a learning culture is suitable for inclusion in this model:

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 ISIMS.

A learning culture can be used to develop effective responses to security incidents when they occur. Organisations often need to adjust the way they operate during or in the immediate aftermath of a cyber-attack, before returning to normal business

operations. The next chapter introduces the concept of a flexible culture, which provides the necessary foundation for this to be achieved.

SECTION 6 FLEXIBLE CULTURE

6.1 WHAT IS A FLEXIBLE CULTURE?

A summary of Reason [53] follows and indicates that a flexible culture is one which is able to effectively adapt to changing demands. A variety of organisations need, as far as practicable, to operate to an error free standard. These organisations often need to manage complex and demanding technology, maintaining their capacity for very high demand and production whilst preventing organisationally destructive failures.

Use of extensively tested Standard Operating Procedures (SOPs) means many of the decisions needed to achieve this can be distilled down to the choice of which SOP to follow. However, SOPs cannot foresee every possible situation or eventuality and an incorrect decision could be detrimental. By establishing a culture where hierarchical positions are relinquished during periods of high intensity operations, in favour of control being deferred to local technical experts, with the rest of the team supporting them, decisions can be made by those most experienced to make them.

By working in such a manner, as well as through sharing of past experiences, the knowledge of many employees can be increased without the need for a trial and error approach to dealing with unanticipated scenarios. Instead, employees can learn from the experts so that when faced with the same or similar non-anticipated scenarios, they have the confidence and expertise to deal with it.

Such flexibility relies on staff knowing their skills and abilities. It relies on management and supervisors with sufficient humility to recognise that they are not always the best person for the job in every circumstance. Leaders need the right training to be invested in them so that they know how to recognise such situations, relinquish and subsequently resume control. It also requires investment in professional skills training for employees, so that the right people with the right expertise are in the right place when the need arises. In short, it requires investment in the training, motivation and experience of the entire workforce.

The MAA hold the view that "*the complex and diverse nature of Defence Aviation dictates that the response to safety concerns be flexible. Rigid adherence to*

inadequate policies will not enable satisfactory resolutions to problems. Policy will evolve to meet challenges presented by the complexities of the Defence Aviation Environment" [42]. A summary of a case study discussed by Duhigg [16], in which the organisation's culture was inflexible, follows.

6.2 SAFETY CASE STUDY

In London on a November evening in 1987, a commuter informed a ticket inspector of a burning tissue at the bottom of a nearby escalator in King's Cross train station. The ticket collector rode to the bottom of the escalator, beat the fire out with a magazine and then returned to his post. He didn't investigate further, tell anyone else or call the fire brigade. Safety was the responsibility of another department and he wasn't aware of who he should tell within the heavily bureaucratic organisation.

The station ran smoothly due to a very delicate balance of power between the heads of various departments and relied on uneasy cooperation between their respective departments and sub-departments. As an investigator later noted, none were likely to trespass on the other's territory, not even to determine if staff were correctly trained in safety matters.

As more reports of smoke came in, the station's safety inspector was called. Following unwritten rules, not having seen the fire himself, he didn't call the fire brigade. A policeman saw flames in a tunnel but had to walk up to street level to use his radio. The policeman's headquarters informed the fire brigade of a fire some twenty two minutes after the burning tissue was first reported.

Sprinkler systems had been installed in the station but nobody knew how to use them. The province of a different department, the demarcation between each meant that people knew their place but were not able to work collaboratively. By the time the first fireman arrived, just under thirty minutes after the ticket inspector was informed about the tissue, the fire was already out of control. Still trains and people kept arriving; only one entrance had been roped off.

Old paint in the stations tunnels had been repeatedly painted over, despite being reported as a hazard by one department but dismissed as meddling by another, and helped fuel the fire. So too did fresh oxygen being pushed ahead of trains arriving in

the tunnels below. Passengers lined the underground platforms, by this time filled with smoke. Train drivers would not re-open doors to let people escape the building heat and fumes because it would have meant causing delays to the train service at other stations.

Just over thirty minutes after the burning tissue was reported the fire reached flashover point; the gasses that had been building ignited. Trapped by the tunnels, the fire eventually exploded into the station's street level ticketing hall, causing the temperature to rise by 150 degrees in half a second.

Six hours later, having been prevented by their own rules from using the station's water hydrants and so having to only use street level hydrants, the fire brigade finally extinguished the fire. Lack of access to blueprints of the station, locked in an office to which nobody had access, hampered the fire brigade's efforts too. Dozens of people had been injured and thirty one were dead.

6.3 ANALYSIS

A flexible culture enables an organisation's staff to be equipped for and deal with unexpected situations or that are out of the ordinary. When such an occasion occurs, there are two ways in which it can be handled.

The first is to effectively ignore the situation, either outright or by taking an immediate action that placates the obvious issue at hand, which is effectively what the ticket inspector did in the preceding example. For instance, the author has previously reported a relatively obvious security flaw to an organisation but was seemingly ignored. A response was received saying the reported flaw would be investigated; yet there has been no obvious change to reflect any consideration being given to the report. Whilst it is impossible, without inside knowledge, to know what actions were taken, if any, an inflexible organisational culture may have contributed to the lack of response.

A second approach is for whoever is first made aware of an abnormal or unexpected situation to either know how to deal with it, or whom should be informed so that it can be dealt with. The rest of the organisation must be suitably configured and trained so that it can quickly adapt to deal with the crisis and then revert to business as normal.

In the King's Cross case study, this would have meant the ticket inspector knowing the necessary safety actions to take in the event of a reported fire. More than that, it would have meant all departments being empowered to utilise their expertise, with lines of communication changing to support this.

In information security, this might mean empowering a customer service agent to report directly to the security team on receipt of a customer's concern that they have been emailed their password, having clicked on a website link for recovering account access. Or it could be that a Security Operations Centre operative, either in-house or provided by a third party, is empowered to dynamically reconfigure security settings because of an alert generated by an organisation's Intrusion Detection System. Whilst the required speed of the response in each of these scenarios may be different, those with the expertise to deal with the demands of the situation need to be authorised to make decisions and act, without always having to check with senior managers, who may not be available or have the requisite knowledge needed to do so.

When experts are having to make decisions, it is important they have access to all relevant information rather than it being locked away. Policies within organisations should reflect this, but should also be reviewed regularly to make sure they are updated. In times of crisis, such as during an ongoing cyber-attack, the personnel managing the situation should have sufficient knowledge to be able to override policy and be aware of the impact of doing so, if they believe such action will be of benefit. There are times to be dogmatic and there are times to override doctrine; the key in doing so is knowing why the doctrine is not suitable for solving the problem at hand. It would be a foolish system's administrator indeed, who, after being told by an ex-employee that disabling their user account would cause a ransomware logic bomb to initiate, goes ahead and disables the account without investigating and taking necessary precautions, just because that is what the company's procedures dictate.

What is also highlighted is that security cannot be a silo, with all related activities contained within it. Instead, it needs to be spread across the breadth and depth of an organisation to be truly effective. Furthermore, staff need to not only be empowered to utilise their knowledge and experience, but also be trained and educated in security related matters and the systems that can be used to help enforce security,

as much of the literature examined in Section 2.1 illustrates. This is especially so if security is not an employee's core area of expertise. Such empowerment also applies to raising concerns or articulating ideas. On no account should suggestions made by one department be dismissed out of hand by another as not being within their purview; such a suggestion may be vital in preventing a security incident and it would be a shame if this was only acknowledged in hindsight, like the contribution painting over old paint made in the case study.

After any instance where the flexibility of an organisation must be exercised in such a way, two things should happen. One, overarching policy should be reviewed to see if amendments need to be made. Two, details of the situation and actions taken to resolve it should be made available to staff. This provides awareness and education, thus increasing employee knowledge – a requirement identified in Section 2.3. Whether this is done immediately or after a period of reflection is mostly immaterial, but in either case, such events should be recorded as per a reporting culture and communicated as per a learning culture.

6.4 SECURITY CASE STUDY

A blog post written by Pen Test Partners [45] describes several security vulnerabilities the company found in a remote-control Aga oven. Whilst the example may be rather contrived, the information explaining their attempts at disclosure are illuminating. With no disclosure process provided on Aga's official website, Pen Test Partners attempted to make contact via email and Twitter but received no response. They attempted to telephone on several occasions but the calls either rang out or were answered by staff who were unaware of how to deal with such issues. The technical team were unable to assist and no directors were available to speak with. Full details of the flaws were eventually published online by Pen Test Partners.

Examples such as this highlight one of two things. Either the organisation just doesn't care or they have a culture which is too rigid. Assuming the latter, by implementing a flexible culture, their employees would have been empowered to deal with the reported flaw in the first instance. Policies covering what services were installed on future devices could have been implemented and it would enable management to realise they ought to invest in providing security training for their

staff, especially their customer service and technical teams. This case study also shows just how necessary security training is for organisations which do not specialise in information security.

6.5 SUMMARY

A flexible culture helps to create a working environment that can respond and evolve to changes in circumstance. The MAA [42] definition, with slight modification, is again a suitable baseline from which to provide a definition of a flexible culture for inclusion in an engaged information security culture:

The complex and diverse nature of Information Security dictates that the response to security concerns be flexible. Rigid adherence to inadequate policies will not enable satisfactory resolutions to problems. Policy will evolve to meet challenges presented by the complexities of the organisation.

The purpose of the values and behaviours components examined so far has been to create an environment conducive to learning from past outcomes and effectively applying these lessons to help reduce the risks of future security incidents and breaches. The final element, a questioning culture, helps to draw these all together.

SECTION 7 QUESTIONING CULTURE

7.1 WHAT IS A QUESTIONING CULTURE?

A questioning culture links just, reporting, learning and flexible cultures. Its purpose is to promote thinking rather than the slavish following of procedures and checklists. It promotes the challenging of assumptions and testing of ideas. It is what enables judgement to be applied rather than assuming safety based on successful historical precedents [25]. This is further expanded on by the MAA, who state that a questioning culture is "*the keystone of a Safety Culture. People and organizations 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 safety culture*" [42].

The final case study is relatively brief and summarises Bromiley [12] and Syed [71]. Most of the relevant points are drawn from the aftermath, although it would not be possible to draw attention to them without some element of context.

7.2 SAFETY CASE STUDY

On 11 April 2005, Emily Bromiley passed away in an Intensive Care Unit (ICU) in a hospital in England. A healthy patient, she had been due to undergo an elective surgery that never took place due to problems that emerged once she was anaesthetised. Despite attempts to prompt them by the nursing staff, doctors did not carry out an emergency procedure and when Emily was finally admitted to ICU it materialised that she would not recover [12].

After being anaesthetised, doctors failed to successfully fit an oxygen mask to provide Emily with air during the procedure. Following protocol, they tried alternative options with no success, but for whatever reasons, did not heed suggestions to conduct an emergency tracheotomy. When the doctors finally managed to restore her oxygen supply they were surprised to learn that twenty minutes had passed [71].

Emily's husband, an airline pilot, wanted an investigation to be conducted so that lessons might be learned to help prevent a similar tragedy befalling anyone else. The investigation revealed that multiple human factors within a failing system combined to turn a potentially salvageable emergency into a tragedy. Ten years on, the

lessons learned are used to teach personnel in industries ranging from engineering to aviation. And healthcare worldwide, an industry with an almost impenetrable culture, has begun to take these lessons on board and make changes in how lessons are identified, communicated and learned from [12].

7.3 ANALYSIS

It is difficult to directly relate a questioning culture to obvious aspects of information security. However, when viewed as the element which binds the previous four cultures together, its importance is hopefully clear. It is necessary to ask hard questions in the wake of an accident, but staff should also be encouraged to do so during the course of a procedure [14] too.

Adherence to procedures and checklists, or SOPs, serve as a valuable aid to routines and processes, but not every eventuality can be covered [53], as has been seen in Section 6.1 and is further highlighted by the doctor's actions in the case study. To that end, people should be encouraged to question why a procedure is conducted in a certain way or at all in a given scenario. Staff should feel comfortable asking to be shown how to carry out operations. And senior employees who are challenged in this way should not perceive it as their authority being threatened but rather have sufficient humility to accept they are not always right [14]. It needs to be remembered that questions challenge assumptions and beliefs and this can be a catalyst for improvement. Questions can also help prevent bad outcomes, provided they are asked and listened to rather than dismissed, as may have been the case when the nurse's recommendation was ignored in the above scenario.

Asking such questions in the heat of the moment can potentially alter the course of a situation, turning an undesirable outcome into one that is tolerable or even desirable. Furthermore, there is greater power in such questions, as can be seen by the reforms to British healthcare, prompted by the efforts of Bromiley in his quest to prevent a similar outcome happening to another person [12].

The case study shows that asking these questions after an event helps to drive reforms, even if the timeframe is somewhat protracted. Perhaps this is not unexpected, since trying to change people's beliefs and assumptions is in effect an attempt at altering their habits. Whilst this is not impossible, it is very difficult since it

relies on being able to identify the reward a person experiences when carrying out a given action in response to some cue, and then changing that action to something new [16]. The topic of habit changing has been well researched in recent years, as Duhigg [16] demonstrates. Although beyond the scope of this thesis, it is an interesting field that may be useful in helping to understand how to change people's information security habits.

7.4 SECURITY CASE STUDY

A whitepaper [74] provides an account of an investigation into an attack vector that could perhaps be considered an urban myth. Dropping almost 300 USB sticks in and around a university, the researchers wanted to see how many were picked up and connected to computers. Each USB stick was configured with non-malicious software that attempted to contact a specific server once connected to a device, which would provide the researchers with the information they needed. Of the USB devices deployed, most were subsequently connected to computers.

Although this was only a study and the USB devices harmless, examples such as this highlight the need for a questioning culture. Whilst not aimed directly at policies or the way things are done, asking why a USB stick would be left lying around and if it is safe to connect it to a computer could help prevent the initial stages of a cyber-attack. Importantly, it also illustrates that unless people have some security knowledge they may not even know that something which is seemingly innocuous should be questioned.

7.5 SUMMARY

A questioning culture is important because it facilitates discussion about what has gone wrong (or right). It can help to reform processes, engage people in learning and provide a platform for improved communication, which Section 2.3 identifies as key considerations for any information security culture framework. These are valuable in their own right, but when combined with just, reporting, learning and flexible cultures and applied in the context of a wider information security culture, can foster organisational change. Adapting the MAA [42] definition for use in an engaged information security culture yields the following:

A questioning culture is the keystone of an information security culture. People and organizations 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.

SECTION 8 UNDERPINNING COMPONENTS

8.1 LEADERSHIP COMMITMENT

As has been seen throughout each of the values and behaviours components, the commitment of an organisation's leaders is a key factor driving the creation and adoption of each culture. The MAA notes "*it is widely accepted that leadership commitment is vital if a successful Safety Culture is to develop within an organization; it is unrealistic to expect the desired culture to flourish if the leadership is not committed to it*" [42].

Haddon-Cave provides a non-exhaustive yet comprehensive list of people who have stressed that leadership is a key element for conducting cultural change within an organisation [25]. It is also recognised as a key component within information security standards [10][11], as well as having been identified as an essential element of an information security culture in Section 2.3.

It is not within the remit of this thesis to conduct an exposé of various leadership styles and how to use them for the creation and ongoing maintenance of each of the just, reporting, learning, flexible and questioning cultures. However, it is worth reiterating that leadership commitment is a vital component in an engaged information security culture, hence it underpins the entire model. The following statement, modified from that given by the MAA [42], reflects this:

It is widely accepted that leadership commitment is vital if a successful information security culture is to develop within an organization; it is unrealistic to expect the desired culture to flourish if the leadership is not committed to it.

8.2 OPEN COMMUNICATION

The need for communication in an engaged information security culture is similar to the requirement to communicate at all stages of the risk assessment process [9][70]. This has been shown in each of the values and behaviours components and its importance is succinctly explained by the MAA: "*clear and unguarded communication of safety related information, throughout all levels of the organization,*

is required if the intelligence contained within such information is going to be exploited to the full" [42].

Open communication is needed by management when communicating their expectations of employees in a just culture, and by staff when reporting errors, mistakes or details of a security breach in a reporting culture. Learning cannot take place if the results of investigations are not clearly propagated within an organisation's learning culture. Neither can flexibility be exercised if poor communication prevents details of arising situations from reaching those with the necessary experience to deal with them. Questions cannot be asked nor answered and assumptions challenged or upheld, limiting ongoing improvements, if staff are restricted in their ability to communicate freely.

Open communication is vital in an engaged information security culture. As an underpinning component, this emphasis is warranted. An adaptation of the MAA statement [42] provides a concise definition:

Clear and unguarded communication of information security related information, throughout all levels of the organization, is required if the intelligence contained within such information is going to be exploited to the full.

8.3 EFFECTIVE DECISION MAKING

Following on from the assertion made in Section 6 that security cannot be conducted in a silo, a fundamental aspect of effective decision making is that information security needs to be a part of every aspect of an organisation. The MAA considers this to be the case in an engaged air safety culture, and notes that "*Air Safety needs to be fully embedded within all aspects of an organizations decision making processes to ensure that the safety impact of any decisions is considered and understood*" [42].

This means information security is included as a first-class citizen on the boards agenda as well as for all employees, and must be considered from the outset and through all stages of project management and business as usual. Despite the best will in the world, this cannot be achieved without effective open communication –

how can a decision be made if leaders do not know the object about which it refers, nor the factors affecting it?

Effective decision making requires knowledge, which is gained through both experience and training. Relevant training can be provided based on learning from reports. Mistakes and key recommendations from security incident investigations have been shown in Section 5 as fertile ground for determining areas where knowledge can be improved. Enhancing education, in turn, serves to provide staff with the necessary expertise to make better decisions.

Embedding information security in all aspects of an organisation ensures that the people with the right knowledge are in the right place to make effective decisions. Effective decision making is thus an important underpinning component of an engaged information security culture, and it can be summed up by an adaptation of the MAA comment [42]:

Information security needs to be fully embedded within all aspects of an organizations decision making processes to ensure that the security impact of any decisions is considered and understood.

SECTION 9 MODEL SUMMARY

Based on the analysis conducted in Section 2.6, the following definition of an engaged information security culture was developed:

> "*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.*"

The model also relies on the revised definition of information security, developed in Section 2.6: "*Information security is the state of freedom from unacceptable risk of loss of information confidentiality, integrity, or availability throughout the life cycle of a system or service. It extends across all organisational areas and addresses resilience to an attack.*"

These definitions were initially used to show how the intent of information security and air safety are sufficiently similar and to justify a more in-depth in investigation and draw comparison. They also provide insight into the overall intent of the framework, which consists of values and behaviours components – just, reporting, learning, flexible and questioning cultures – and underpinning components – leadership commitment, open communication and effective decision making. The analogy given in Section 2.2 that any such model ought to be like a blueprint for a house is reinforced by Figure 9-1, which provides a visual overview of the final model and is developed from Figure 2-2.

The concept of a just culture was explored in Section 3 and yielded the following definition:

> "*All personnel must understand that honest errors can be made and a just culture 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."

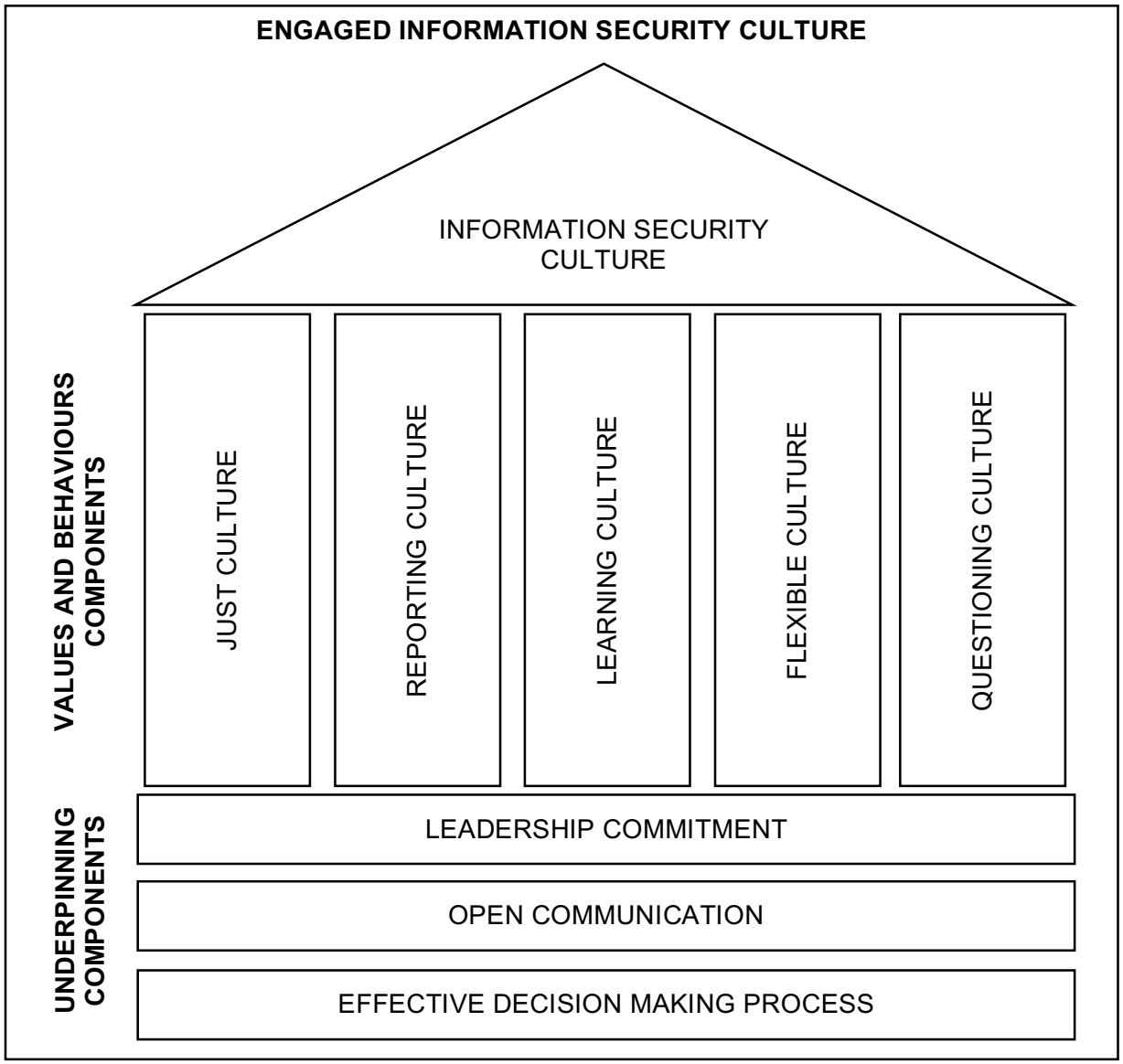

Figure 9-1: Model for an Engaged Information Security Culture

Next, in Section 4, a reporting culture was considered and defined. A reporting culture acknowledges:

"*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 ISMS are vital for a healthy reporting culture.*"

Building on the ideas of just and reporting cultures, Section 5 determined that a learning culture means:

> "*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 ISIMS.*"

Following this, Section 6 examined what a flexible culture means and determined:

> "*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.*"

Finally, Section 7 explored the concept of a questioning culture:

> "*A questioning culture is the keystone of an information security culture. People and organizations 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.*"

After considering each of the values and behaviours components, the underpinning components were addressed in turn. Each of these aspects are central to each of the sub-cultures.

Section 8.1 reviewed what is meant by leadership commitment:

> "*It is widely accepted that leadership commitment is vital if a successful information security culture is to develop within an organization; it is unrealistic to expect the desired culture to flourish if the leadership is not committed to it.*"

Next open communication was considered in Section 8.2:

> "*Clear and unguarded communication of information security related information, throughout all levels of the organization, is required if the intelligence contained within such information is going to be exploited to the full.*"

Lastly, Section 8.3 examined effective decision making, concluding that:

> "*Information security needs to be fully embedded within all aspects of an organizations decision making processes to ensure that the security impact of any decisions is considered and understood.*"

Together, the five values and behaviours components sub-cultures, along with each of the underlying components, form the framework for an engaged information security culture. Each is of equal importance; if any are omitted, the result will be an ineffective model.

SECTION 10 CONCLUSION

This project has investigated safety culture as a basis from which to develop a model for information security culture. Having been identified as a possible method in the author's literature review in Section 2.1, such an approach has not been taken or obviously discounted previously. Previous research has instead focused on how models for defining organisational culture can be adapted and expanded to encompass information security. From this research, several key requirements for any information security culture framework were identified.

By considering how safety culture is employed in various safety critical industries, predominantly but not exclusively aviation and healthcare, and reasoning that the objectives of organisations in such industries are sufficiently similar to information security related objectives, this project has shown that there is enough commonality to use safety culture as a basis for defining information security culture. For example, the MAA's introduction of an engaged air safety culture includes objectives such as foster improvements by learning from mistakes, encourage knowledge sharing, reduce risk arising from errors, and promote leadership commitment. These are parallel ambitions to those of information security management. While the author acknowledges that safety culture and information security differ in some areas, the increasing convergence of information technology and operational technology and the rise of the IoT provide further justification for such a model forming the basis from which to explore the components of an engaged information security culture.

With this foundation in place, each values and behaviours component – just, reporting, learning, flexible and questioning cultures – of the underlying model was explored in detail. Each concept was explained and followed by a case study from a safety related industry, which was subsequently analysed and lessons applicable to information security identified. These lessons were then linked to the previously established key requirements. Finally, a brief case study explaining how these lessons could relate to information security was presented. After considering each of these aspects, the underpinning components of leadership commitment, open communication and effective decision making were studied. This enabled a final model to be defined, which was presented in Section 9.

Although this model has been developed by taking a different approach to those taken in the existing literature, it is important to note that the initial review highlighted several points of commonality in the findings of those studies. This model remains consistent with those common points. Furthermore, it is consistent with existing information security related standards, such as those in ISO/IEC 27000 series [11][10]. To illustrate a few examples, there is parity in the need for leadership commitment, implementing a process to monitor and review risks, and to have an information security culture, the latter of which is obviously the focus of this project. Other common information security practices such as SIEM, the exploitation of threat intelligence, and use of existing security awareness training can be incorporated into the model.

As has been shown, successfully tackling the challenges of modern information security needs more than just employing technical controls. It requires a dedicated approach that is consistent across organisations, understood by all employees and adapts to meet changes in circumstances. Adopting an engaged information security culture as defined in this report is a means to help in this regard.

Some of the failures in information security as outlined in Section 1 were likened in Section 2.5 to a catastrophic safety failure in terms of severity. Such comparisons are perhaps slightly disingenuous. However, it is hopefully clear that an accident similar in scale to that of the King's Cross fire (Section 6.2) or the Nimrod crash (Section 2.5), caused by a failure in information security, should not be the initial catalyst for change.

It is the author's opinion that the adoption of a model for an engaged information security culture is most likely to begin with industries who already have experience of operating within a safety culture. Such a view is held predominantly due to the convergence of connected systems with safety critical applications. Should this prediction be correct, hopefully those industries will be able to demonstrate the benefits of such a culture, leading to its adoption across a wider spectrum of organisations.

Finally, it is worth noting that the model presented in this report has not been subject to rigorous academic evaluation. Based on subjective comparison and logical reasoning, its principles could be employed today, but further scrutiny from within

academic and business spheres would enhance it. As an absolute minimum, it provides details of a valuable alternative framework for information security culture that both augments and challenges the thinking of existing research.

BIBLIOGRAPHY

1. Areej AlHogail. 2015. Design and validation of information security culture framework. *Computers in Human Behavior* 49, (Aug. 2015), 567–575. DOI:https://doi.org/10.1016/j.chb.2015.03.054.
2. Mohammed A. Alnatheer. 2014. A Conceptual Model to Understand Information Security Culture. *International Journal of Social Science and Humanity* 4, 2 (Mar. 2014), 104–107. DOI:https://doi.org/10.7763/IJSSH.2014.V4.327.
3. Saad Haj Bakry. 2003. Development of security policies for private networks. *International Journal of Network Management* 13, 3 (May/Jun. 2003), 203–210. DOI:https://doi.org/10.1002/nem.472.
4. BBC News. 2006. 14 UK troops die in Afghan crash. *BBC News*. Retrieved January 4, 2017 from http://news.bbc.co.uk/1/hi/world/south_asia/5308622.stm.
5. BBC News. 2008. RAF Nimrod's last moments heard. *BBC News*. Retrieved January 4, 2017 from http://news.bbc.co.uk/1/hi/uk/7386975.stm.
6. BBC News. 2008. Nimrod victims' families sue MoD. *BBC News*. Retrieved January 4, 2017 from http://news.bbc.co.uk/1/hi/uk/7797582.stm.
7. John Bingham. 2009. MoD admits responsibility for Afghanistan Nimrod explosion deaths. *The Telegraph*. Retrieved January 4, 2017 from http://www.telegraph.co.uk/news/uknews/defence/5071466/MoD-admits-responsibility-for-Afghanistan-Nimrod-explosion-deaths.html.
8. Kelly Bissell, Ryan LaSalle, and Kevin Richards. 2017. The Cyber-Committed CEO. *Accenture*. Retrieved March 9, 2017 from https://www.accenture.com/us-en/insight-cyber-committed-ceo.
9. British Standards Institution. 2011. *BS ISO/IEC 27005:2011: Information Technology - Seurity Techniques - Information Security Risk Management*. British Standards Institution, London, UK.
10. British Standards Institution. 2013. *BS ISO/IEC 27001:2013: Information Technology - Security Techniques - Information Security Management Systems - Requirements*. British Standards Institution, London, UK.
11. British Standards Institution. 2016. *BS ISO/IEC 27000:2016: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*. British Standards Institution, London, UK.
12. Martin Bromiley. 2015. The husband's story: from tragedy to learning and action. *BMJ Quality & Safety* 24, 7 (Jul. 2015), 425–427. DOI:https://doi.org/10.1136/bmjqs-2015-004129.
13. Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. 2017. Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior* 67, (Feb. 2017), 196–206. DOI:https://doi.org/10.1016/j.chb.2016.10.025.
14. Sidney Dekker. 2012. *Just culture: balancing safety and accountability (2nd. ed.)*. CRC Press, Farnham, UK.

15. James R. Detert, Roger G. Schroeder, and John J. Mauriel. 2000. A Framework for Linking Culture and Improvement Initiatives in Organizations. *The Academy of Management Review* 25, 4 (Oct. 2000), 850–863. DOI:https://doi.org/10.2307/259210.

16. Charles Duhigg. 2013. *The power of habit: why we do what we do and how to change*. Random House Books, London, UK.

17. FireEye. 2017. Advanced Persistent Threat Groups. *FireEye*. Retrieved June 2, 2017 from https://www.fireeye.com/current-threats/apt-groups.html.

18. Conner Forrest. 2016. Dyn DDoS attack: 5 takeaways on what we know and why it matters. *TechRepublic*. Retrieved March 11, 2017 from http://www.techrepublic.com/article/dyn-ddos-attack-5-takeaways-on-what-we-know-and-why-it-matters/.

19. Conner Forrest. 2016. How the Mirai botnet almost took down an entire country, and what your business can learn. *TechRepublic*. Retrieved January 7, 2017 from http://www.techrepublic.com/article/how-the-mirai-botnet-almost-took-down-an-entire-country-and-what-your-business-can-learn/.

20. Liam Fox. 2010. Charter for the United Kingdom Military Aviation Authority. *GOV.UK*. Retrieved January 4, 2017 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/335845/Maa_charter.pdf.

21. Sean Gallagher. 2016. San Francisco public transport system locked up by ransomware attack. *Ars Technica UK*. Retrieved June 2, 2017 from https://arstechnica.co.uk/security/2016/11/san-francisco-muni-ransomware-attack/.

22. Gemalto. 2017. Data Breach Statistics by Year, Industry, More. *Breach Level Index*. Retrieved June 2, 2017 from http://breachlevelindex.com.

23. Samuel Gibbs. 2016. Dropbox hack leads to leaking of 68m user passwords on the internet. *The Guardian*. Retrieved January 7, 2017 from https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach.

24. Chris Graham. 2017. NHS cyber attack: Everything you need to know about “biggest ransomware” offensive in history. *The Telegraph*. Retrieved June 2, 2017 from http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

25. Charles Haddon-Cave QC. 2009. *The Nimrod Review*. Retrieved January 4, 2017 from https://www.gov.uk/government/publications/the-nimrod-review.

26. Rita Heimes. 2016. Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification. *International Association of Privacy Professionals*. Retrieved January 4, 2017 from https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/.

27. Information Commissioner’s Office. 2016. TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack. *Information Commissioner’s Office*. Retrieved January 7, 2017 from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/.

28. Information Commissioner's Office. 2016. Overview of the General Data Protection Regulation (GDPR). *Information Commissioner's Office*. Retrieved November 2, 2016 from https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.
29. International Civil Aviation Organisation. 2013. *Safety Management Manual (SMM) (3rd. ed.)*. International Civil Aviation Organisation, Montréal, Canada.
30. John T. James. 2013. A New, Evidence-based Estimate of Patient Harms Associated with Hospital Care. *Journal of Patient Safety* 9, 3 (Sep. 2013), 122–128. DOI:https://doi.org/10.1097/PTS.0b013e3182948a69.
31. Eamon Javers. 2013. Why Companies Keep Quiet About Cyberattacks. *CNBC*. Retrieved November 7, 2016 from http://www.cnbc.com/id/100491610.
32. Michael Kassner. 2009. 10 ways to avoid IT security breaches. *TechRepublic*. Retrieved March 11, 2017 from http://www.techrepublic.com/blog/10-things/-10-ways-to-avoid-it-security-breaches/.
33. Brian Krebs. 2016. KrebsOnSecurity Hit With Record DDoS. *Krebs on Security*. Retrieved January 7, 2017 from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.
34. Brian Krebs. 2016. DDoS on Dyn Impacts Twitter, Spotify, Reddit. *Krebs on Security*. Retrieved January 7, 2017 from https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.
35. Brian Krebs. 2017. U.K. Hospitals Hit in Widespread Ransomware Attack. *Krebs on Security*. Retrieved June 2, 2017 from https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/.
36. Brian Larder. 2002. *CAA Paper 2002/02: Final Report on the Helicopter Operations Monitoring Programme (HOMP) Trial*. Retrieved February 20, 2017 from http://www.eurohoc.org/task/task_docs/CAPAP2002_02.pdf.
37. Tyson Macaulay and Bryan Singer. 2012. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, Boca Raton, FL.
38. Malwarebytes Labs. 2016. Security in 2017: Ransomware will remain king. *Malwarebytes Labs*. Retrieved June 2, 2017 from https://blog.malwarebytes.com/threat-analysis/2016/12/security-in-2017-ransomware-will-remain-king/.
39. Keith M Martin. 2012. *Everyday Cryptography: Fundamental Principles and Applications*. Oxford University Press, Oxford, UK.
40. McAfee Labs. 2016. 2017 Threats Predictions. *McAfee*. Retrieved January 7, 2017 from http://www.mcafee.com/au/security-awareness/articles/mcafee-labs-threats-predictions-2017.aspx.
41. Joseph Menn. 2015. Companies Do Not Report Hacking - Digital Workplace - Grand Valley State University. *Grand Valley State University*. Retrieved November 7, 2016 from https://www.gvsu.edu/e-hr/companies-do-not-report-hacking-60.htm.
42. Military Aviation Authority. 2015. Manual of Air Safety - MAS. *GOV.UK*. Retrieved January 10, 2017 from

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/577618/MAS_Issue_5.pdf.

43. Johan van Niekerk and Rossouw von Solms. 2010. Information security culture: A management perspective. *Computers & Security* 29, 4 (Jun. 2010), 476–486. DOI:https://doi.org/10.1016/j.cose.2009.10.005.
44. Evgeniya O'Regan Pevchikh. 2015. *Information Security Culture: Definition, Frameworks and Assessment: A Systematic Literature Review*. Master's Thesis. Luleå University of Technology, Luleå, Sweden. Retrieved January 26, 2017 from http://ltu.diva-portal.org/smash/get/diva2:1019291/FULLTEXT02.pdf.
45. Pen Test Partners. 2017. IoT Aga. Cast iron Security Flaw. *Pen Test Partners*. Retrieved June 2, 2017 from https://www.pentestpartners.com/security-blog/iot-aga-cast-iron-security-flaw/.
46. PhishTank. 2017. Frequently Asked Questions (FAQ). *PhishTank*. Retrieved June 2, 2017 from http://www.phishtank.com/faq.php.
47. PhishTank. 2017. Friends of PhishTank. *PhishTank*. Retrieved June 2, 2017 from http://www.phishtank.com/friends.php.
48. Peter Pronovost. 2014. *Hearing Patient Safety*. Video. (17 July 2014). Retrieved January 7, 2017 from https://www.c-span.org/video/?320495-1/hearing-patient-safety.
49. Protiviti. 2017. Managing the Crown Jewels and Other Critical Data. *Protiviti*. Retrieved March 9, 2017 from https://www.protiviti.com/US-en/insights/it-security-survey.
50. Robert Radvanovsky and Jacob Brodsky. 2016. *Handbook of SCADA/Control Systems Security*. CRC Press, Boca Raton, FL.
51. James Reason. 1998. Achieving a Safe Culture: Theory and Practice. *Work & Stress* 12, 3 (Sep. 1998), 293–306. DOI:https://doi.org/10.1080/02678379808256868.
52. James T. Reason. 1990. *Human Error*. Cambridge University Press, Cambridge, UK.
53. James T. Reason. 1997. *Managing the Risks of Organizational Accidents*. Ashgate, Farnham, UK.
54. James T Reason. 2016. *Organizational Accidents Revisited*. Ashgate, Farnham, UK.
55. Tim Robinson. 2012. Empowering military air safety. *Royal Aeronautical Society*. Retrieved January 4, 2017 from https://www.aerosociety.com/news/empowering-military-air-safety/.
56. Anthonie B. Ruighaver and Sean B. Maynard. 2006. Organizational Security Culture: More Than Just an End-User Phenomenon. In *Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006)*. Springer, Boston, MA, 425–430. DOI:https://doi.org/10.1007/0-387-33406-8_36.
57. Nader Sohrabi Safa and Rossouw von Solms. 2016. An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior* 57, (Apr. 2016), 442–451. DOI:https://doi.org/10.1016/j.chb.2015.12.037.

58. Anne Saita. 2013. “Terrific Employee” Fired After Losing USB Drive Containing Medical Records. *Threatpost*. Retrieved June 2, 2017 from https://threatpost.com/terrific-employee-fired-after-losing-usb-drive-containing-medical-records-011713/77422/.

59. Sameer. 2017. LastPass 2FA Bug Reported & Resolved. *The LastPass Blog*. Retrieved June 2, 2017 from https://blog.lastpass.com/2017/04/lastpass-2fa-bug-reported-resolved.html/.

60. Joel Schectman. 2014. When to Disclose A Data Breach: How About Never? *The Wall Street Journal*. Retrieved July 11, 2016 from http://blogs.wsj.com/riskandcompliance/2014/03/27/when-to-disclose-a-data-breach-how-about-never/.

61. Edgar H Schein. 1985. *Organizational culture and Leadership*. Jossey-Bass Publishers, San Francisco, CA.

62. Thomas Schlienger and Stephanie Teufel. 2002. Information Security Culture. In *Security in the Information Society*. Springer US, New York, NY, 191–201. DOI:https://doi.org/10.1007/978-0-387-35586-3_15.

63. Thomas Schlienger and Stephanie Teufel. 2003. Analyzing information security culture: increased trust by an appropriate information security culture. In *14th International Workshop on Database and Expert Systems Applications, 2003 Proceedings*. IEEE, Los Alamitos, CA, 405–409. DOI:https://doi.org/10.1109/DEXA.2003.1232055.

64. Thomas Schlienger and Stephanie Teufel. 2003. Information security culture - from analysis to change : research article. *South African Computer Journal* 2003, 31 (Dec. 2003), 46–52. Retrieved January 26, 2017 from http://hdl.handle.net/10520/EJC27949.

65. Cory Scott. 2016. Protecting Our Members. *LinkedIn Official Blog*. Retrieved January 7, 2017 from https://blog.linkedin.com/2016/05/18/protecting-our-members.

66. Joe Siegrist. 2015. LastPass Security Notice. *The LastPass Blog*. Retrieved June 2, 2017 from https://blog.lastpass.com/2015/06/lastpass-security-notice.html/.

67. Joe Siegrist. 2017. Security Update for the LastPass Extension. *The LastPass Blog*. Retrieved June 2, 2017 from https://blog.lastpass.com/2017/03/security-update-for-the-lastpass-extension.html/.

68. Andrew Simpson. 2016. *Whither the privacy breach case studies?* Department of Computer Science, University of Oxford, Oxford, UK. Retrieved November 4, 2016 from http://www.cs.ox.ac.uk/files/8239/CS-RR-16-06%20-%20Merged.pdf.

69. Splunk. 2017. Analytics-Driven SIEM. *Splunk Enterprise Security*. Retrieved March 11, 2017 from https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security.html.

70. David Sutton. 2015. *Information Risk Management*. BCS Learning & Development Limited, Swindon, UK.

71. Matthew Syed. 2016. *Black Box Thinking: Marginal Gains and the Secrets of High Performance*. John Murray (Publishers), London, UK.

72. Sam Thielman. 2016. Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*. Retrieved January 7, 2017 from https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

73. Kerry-Lynn Thomson, Rossouw von Solms, and Lynette Louw. 2006. Cultivating an organizational information security culture. *Computer Fraud & Security* 2006, 10 (Oct. 2006), 7–11. DOI:https://doi.org/10.1016/S1361-3723(06)70430-4.

74. Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, and Michael Bailey. 2016. Users Really Do Plug in USB Drives They Find. In *2016 IEEE Symposium on Security and Privacy Proceedings*. IEEE, Los Alamitos, CA, 306–319. DOI:https://doi.org/10.1109/SP.2016.26.

75. Adele da Veiga and Jan H. P. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29, 2 (Mar. 2010), 196–207. DOI:https://doi.org/10.1016/j.cose.2009.09.002.

76. Adele da Veiga and Nico Martins. 2015. An Information Security Culture Model Validated with Structural Equation Modelling. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance*. Plymouth University, Plymouth, UK, 11–21. Retrieved January 26, 2017 from http://uir.unisa.ac.za/handle/10500/19061.

77. Verizon. 2009. The Verizon DBIR: Strengthen Your Defense. *Verizon Enterprise Solutions*. Retrieved January 7, 2017 from http://www.verizonenterprise.com/verizon-insights-lab/dbir/.

78. Verizon. 2016. 2016 Data Breach Investigations Report. *Verizon Enterprise Solutions*. Retrieved January 7, 2017 from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

79. Gonzalo Viña. 2016. Patients in limbo as cyber attack shuts three hospitals. *Financial Times*. Retrieved November 8, 2016 from https://www.ft.com/content/1292d25c-a12a-11e6-891e-abe238dee8e2.

80. Harry Yorke. 2017. Devon town council held to ransom for £3,000 by hackers over return of its allotment waiting lists. *The Telegraph*. Retrieved June 2, 2017 from http://www.telegraph.co.uk/news/2017/02/06/devon-town-council-held-ransom-3k-hackers-return-allotment-waiting/.