Chapter 9
The Role of Security Culture

Jo Malcolmson
QinetiQ Ltd, UK

ABSTRACT

This chapter provides a discussion of the importance of the wider organisational context that the network administrator needs to deal with by describing how the organisational culture can impact on the degree to which security can be successfully maintained. It starts with an acknowledgement of the general clusters of factors that affect security (technology, processes, organisational, and human), and focuses on the human element within these. The types of risk that arise from humans in the system are described, such as motivation, ability, awareness (and lack of awareness). Errors and purposeful violations are compared, and individual, organisational, and latent risk factors explained. The chapter's key focus is the role of organisational culture. A general description of culture and its application in organisations leads into a discussion of security culture. A comparison is made between safety and security culture. Similarities are listed as the impacts of regulatory influence, reputational damage, having multiple causes, and the fact both are often driven by adverse events. Differences are examined. For example, the victim of a poor safety culture is often the perpetrator, whereas this is less often true in security violations. Intrinsic motivation and the impact of certain systems designs are further differences. Gaps in security culture research are noted as a lack of an accepted practical definition, a lack of an accepted way of measuring security culture that can be used outside narrow domains, research into engendering and enhancing security culture is narrowly focused on specific aspects of culture, and a lack of research relating security culture to organisational performance. A project to address some of these gaps by defining and measuring security culture is described. Qualitative and quantitative research was used to develop a questionnaire consisting of seven scales and fourteen sub-scales, each measuring a reliable and distinct factor. The content of these factors is noted, and a case study of the questionnaire's application to facilitate the development of security culture is outlined. Two key benefits result from the use of the questionnaire: diagnosis of aspects of security culture that may need improvement and benchmarking within (and between) organisations.

INTRODUCTION

This chapter begins by defining the risks to security that arises from the human in the system, and describing these in context.

Organisational performance is generally assumed to be a function of its whole system: technology, processes, and people. When designing technology and processes, managers are primarily concerned to ensure that these support

DOI: 10.4018/978-1-4666-8111-8.ch009

the organisation's goals. Put simply, commercial organisations are designed first and foremost to make a profit, by producing goods or services, while public organisations generally provide a service. Therefore, technology and processes created in support of these aims will usually enable easy communications with potential customers/users, capture sales data, and so on.

Whilst the security of the processes and technology can be vital to organisational performance, it is rarely the case that security is of itself a primary aim: instead, security is a supporting driver, and this affects the level of significance that is attributed to it. Elements of the system are expected to provide protection against security breaches without this impacting on performance. In his book *Managing the Risks of Organisational Accidents*, James Reason (1997) describes the relationship between production and protection. He describes a "parity zone" (Reason, 1997, p.3) in which the level of protection matches the hazards of production. Outside this parity zone, it is possible to set the level of protection either too high, or too low, with both having adverse effects on the organisation. While Reason applies these concepts to safety, the conclusions are true for security also. Where protection is too high, a system may be so secure that it prevents or delays communication or some other activity that is essential to production. Where it is too low, it allows a security breach, and associated problems. Organisations are always at some risk of setting the security protection wrongly.

It is assumed that the contribution of technology and processes to security are covered in other chapters in this book, and elsewhere. This chapter focuses on the contribution of people and organisational culture to security. In it, I will argue that just as technology and processes are focused primarily to address other organisational aims, so too are people, and it should therefore be unsurprising that people chosen for their communications skills or ability to produce goods rapidly may not also be naturally focused on security. And just as a process may be set outside the "parity zone," it is also the case that staff (individually and collectively) can have an inappropriate view of the balance between the production and security needs of the organisation, that causes them to behave in a way that negatively impacts on security. These, and other factors that drive human behaviour, will be discussed.

This chapter therefore has a number of objectives. First, it will discuss the types of risk that arise from the human in the system, with a specific focus on organisational culture. Second, the role of culture in affecting organisational outcomes will be set out. Third, the commonalities and differences between security culture and safety culture will be set out. Specific research on security culture has been limited, while safety culture has attracted much interest. Researchers have proposed that there are some parallels between the two: so comparisons are worthy of consideration and an attempt to set out some of the fundamentals of this debate will be made. Fourth, a case study will be described, illustrating some key messages. These include how to define and describe security culture; how to measure it; and a practical example of data analysis and identification of actions needed for improvement.

HUMAN RISKS

The human in the system creates a number of types of risk. Whilst much has been written about outsiders who hack into organisations directly, they are not the focus of this chapter. Instead, I will focus on employees themselves. They may breach security either intentionally, or unintentionally, and knowingly or unknowingly. Both ability and motivational factors are important, and in addition to the impact of individuals, the impact of humans collectively must be considered. The organisational culture influences to what extent individuals deploy their abilities, and in what ways they are willing to do so.