Chapter XXII
Practical Action and Mindfulness in Health Information Security

Jeff Collmann
Georgetown University Medical Center, USA

Ted Cooper
Stanford University Medical Center, USA

ABSTRACT

Although it is sometimes tempting to treat information security as a domain of its own, this approach will inevitably yield failures of information security and failures for the organization. This occurs because serious breaches may originate from organizational conditions not obviously related to information security policies, procedures or practices and because information security practices operate in, and are affected by the context of their parent organization. For these reasons, healthcare leaders must comply with but look beyond good industry practices alone while planning, implementing, and evaluating information security programs. In this chapter, we demonstrate that a consensus exists on key good information security measures that all healthcare leaders should, and often do use in designing their information security programs. We follow this analysis with two case studies that demonstrate the limitations of focusing only on good information security practices. These case studies help explain the mutual interaction between health information security programs and their wider organizational context by introducing key concepts about organizational performance, including "practical action," "practical resistance," "sponsored social movement," and "mindfulness" and examining them at the individual, group, organizational, and cross domain levels of organizational life.

INTRODUCTION

Health care leaders and staff members have spent several years now designing, implementing and evaluating programs for complying with the privacy and security regulations of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Department of Health and Human Services

[HHS], 2000, 2003; Gostin, Turekbrezina, Powers et al 1993; Mandl, Kohane and Brandt 1993). This work typically entails deploying traditional safeguards for information privacy and security on which wide consensus exists. As health care leaders reflect upon their work, however, they should begin looking beyond the boundaries of the traditional information security domain to include insights from the social science literature on High Reliability Organizations (HROs) and organizational failure. Two concepts, practical action and mindfulness may offer particular help in better understanding and trying to learn from their experiences with HIPAA compliance. Scott Snook introduces the concept of "practical action" in his explanation of the friendly fire shoot down of two American helicopters by two American F-15 jets over Northern Iraq during Operation Provide Comfort. According to Snook (2000), "practical action" operates as a ubiquitous feature of organizational life and refers to "behavior that is locally efficient, acquired in practice and legitimized through unremarkable repetition" (p. 182). Weick and Sutcliffe (2001) describe mindfulness in their analysis of avoiding failure in complex organizations faced with the high possibility of unexpected, catastrophic events. From the perspective of Weick, Sutcliffe and Obstefeld (1999), organizations that develop and sustain a state of collective mindfulness create "a rich awareness of discriminatory detail and (facilitate) the discovery and correction of errors capable of escalation into catastrophe." (p.81) Expanding their focus beyond the domain of information security alone will help healthcare executives identify potential vulnerabilities and sources of failure that standard approaches to information protection ignore.

RESEARCH DESIGN AND METHODS

We designed this project to illustrate the necessity for evaluating broad organizational conditions as well as industrial guidelines for good practice in information security planning. Thus, we begin by analyzing current surveys in English of information security practice and comparing them with two important information security initiatives of the United States (US), the Federal Information Security Management Act (FISMA) of 2002 and Security Standard of the Health Insurance Portability and Accountability Act (HIPAA)of 1996 (HHS 2003). This analysis demonstrates that a consensus exists on key good information security measures that all healthcare leaders should, and often do use in designing their information security programs. We follow this analysis with two case studies in the design and implementation of good information security practices across two large organizations, the United Kingdom National Health Service and the US Military Health System. These case studies introduce concepts for and demonstrate the importance of understanding the organizational context for implementing good information security practice. Drawing from the work of Scott Snook (2000), we consider efforts to reform healthcare information security practice at the individual, group and organizational levels of action as well as across levels in the case studies.

TRADITIONAL INFORMATION PROTECTION SAFEGUARDS

With the wide-spread use and integration of information technology into the operations of most organizations, failures in information security have commonly compromised operations, resulted in financial losses and besmirched reputations. To improve information technology security, a body of knowledge has developed that includes policies, procedures, best practices and administrative, physical and technical controls. This body of knowledge has been codified in a number of places including: 1. *An Introduction to Computer Security: The NIST Handbook* (National Institute