Toward a U.S. Army Cyber Security Culture

Christopher Paul, RAND, USA

Isaac R. Porche III, RAND, USA

ABSTRACT

One of the reasons offered for gaps in organizations' cyber security is the lack of a "cyber security culture." This article defines and explores the concept of cyber security culture within the context of the U.S. Army. It concludes that the Army would benefit from the creation and adoption of a cyber security culture, though it would not be a security panacea. The article concludes by identifying and describing important elements of such a culture and practical advice for approaching culture change. These include: the development of policies that can be understood, adhered to, and enforced; change management efforts that unfreeze current culture, seek change, then refreeze/institutionalize changes; a structure that offers incentives for desired behaviors but also identifies and enforces compliance; and change efforts that emphasize change in knowledge/awareness and in attitude.

Keywords: *Change Management, Cyber Security, Cyber Security Culture, Cyberwarfare, Human Dimension, Leadership, Organizational Culture, Security Policy*

INTRODUCTION

Cyber security lags desired levels in much of industry, in governments, and in militaries, including the U.S. Army. One reason offered for this gap is the lack of a "cyber security culture" in many of these organizations. This article explores and defines the notion of an Army cyber security culture, discuses the benefits that could accrue from the establishment of an Army cyber security culture, and identifies barriers to the establishment of such a culture in the U.S. Army. We then discuss successful practices from industry that are applicable to U.S. Army efforts to move from the baseline state, overcoming various existing cultural barriers, and establishing an Army cyber security culture. The discussion includes the importance of security policy, the scope of security culture, the importance of and connected nature of user knowledge and user attitudes, the importance of incentives and accountability, the critical role played by leadership, and relevant practical advice from corporate experiences in change management. This article concludes with examples of successful culture change in the military context: the inclusion of women at West Point and the reform of the nuclear security culture in the 8th Air Force.

DOI: 10.4018/ijcwt.2011070105

DEFINING CYBER SECURITY CULTURE

"Culture" is put to many different uses in research and discussion. Just looking at mentions of "Army culture," one can easily find examples of "culture" being used as shorthand for training and doctrine (Marquez, 2008); to refer to doctrine, organization, and promotion criteria (Campbell, 2007); or to describe other, wholly different concepts.

For our working definition of cyber security culture, we draw on two sources. First, the literature on organizational culture, which fairly uniformly follows Edgar Schein (1992) in defining culture as "[a] pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems" (p. 12).

Second, we draw on the literature on information security, which considers a security culture to be something that is either present or absent in an organization, instead of talking about culture broadly as something that exists and has different features or content depending on the context. For example, Schlienger and Teufel (2003) define an information security culture as something that "should support all activities in such a way that information security becomes a natural aspect in the daily activities of every employee. Security Culture helps to build the necessary trust between the different actors" (p. 405).

Synthesizing these two approaches to discussing culture, throughout this discussion we define an *Army cyber security culture* as follows: "A pattern of shared basic assumptions that supports information security becoming a natural aspect of the daily activities of all Army personnel who operate in cyberspace."

Why Pursue an Army Cyber Security Culture?

There is broad consensus that organizational improvement hinges heavily on effective culture change (Cameron & Quinn, 2006; O'Donovan, 2006). This consensus clearly extends to the area of information security (Rotvold, 2008). As van Niekerk and von Solms (2009) note, "It has become widely accepted that the establishment of an organizational sub-culture of information security is key to managing the human factors involved in information security" (p. 1).

Interest in improving cyber security through changes in organizational culture or the creation of a cyber security culture extends to the U.S. Department of Defense. In 2009, Deputy Defense Secretary William Lynn II indicated in his remarks at a conference that in order to meet cyber threats, DoD must make changes in the "three C's—culture, capability, and command" (Chabrow, 2009, p. 1).

The emphasis on culture as an aspect of cyber security stems primarily from one of the persistent sources of network vulnerability, the "human dimension." Numerous studies point out human behavioral vulnerabilities in cyber security (Rotvold, 2008; Rowe, 2008; van Niekerk & von Solms, 2005). It follows, then, that if the human dimension (users) is a significant source of cyber vulnerability, creating a culture by which *a pattern of shared basic assumptions supports information security becoming a natural aspect of the daily activities of all Army personnel who operate in cyberspace* is a step toward a solution.

Benefits of Establishing an Army Cyber Security Culture

What would the U.S. Army get from the successful establishment of a cyber security culture? Would human-factor vulnerabilities be completely eliminated? No. In the words of U.S. Air Force Colonel Rich Moorehead (R.