Chapter 3
Always on Guard: How a Corporate Immune System Can Engage Full-Spectrum Risks – A Conceptual Framework to Re-Engineer Organizational Capability and Culture

Milyan (Mils) Hills
University of Northampton, UK

ABSTRACT

This chapter advances the idea that the modern organization can become immune to a full spectrum of risks by re-engineering its organizational capability and culture. Given the accepted role of people in causing or escalating technical risk – the requirement to achieve ‘always on’ socio-technical protection poses a significant challenge. However, an enterprise’s human resources offer a massive potential to detect and report risk and there is also substantial competitive advantage available to the organization which develops, integrates, leverages and acts on intelligence gained from a suite of socio-technical sensors and sense-making processes. The human resources and culture of an organization, properly configured, could comprise a powerful innate (constant) and adaptive (active) immune system. The chapter will provide the reader with a framework for how such an immune capability could be integrated into an organization that takes seriously the requirement to be ‘always on’ – protected from any form or blend of socio-technical threat.

DOI: 10.4018/978-1-5225-3704-5.ch003

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

This book is charged with providing readers with conceptual and implementational frameworks to enable them to enhance their organizations’ ability to deliver ‘always on’ availability, and (therefore) to avoid economic, reputational, opportunity and other costs. This chapter seeks to make a substantive and pragmatic contribution to the ability of businesses and other institutions to leverage and harden their defense against a significant cause of cyber-security breaches: people. More positively, rather than seeing the employees, contractors, visitors and customers of an enterprise merely and exclusively as a source of insider threat and other risk – and drawing on my background as a corporate and security anthropologist - this chapter suggests that these individuals enmeshed in an appropriate organizational culture can constitute a corporate immune system.

People can avoid risks, detect unusual events, trigger appropriate responses and learn from both past exposures to challenge and developing immunizations to harden protection and evade infection. And, of course, the immense benefit of a biological immune system – which organizations would desire to have – is that all of its actions occur automatically and without the investment of cognitive effort. To adopt a military, doctrinal term – components of the immune system have “mission command” to act in the best interests of the organism. Innate and active structures and systems form a shield and response capability which are always on duty.

Of course, when we as individuals are sick - we seek expert assistance to help aid our recovery (prioritize our survival and wellbeing, prevent us from transmitting our illness to others) and therefore invest cognitive effort to do this. Likewise, in the world of the bureaucratic institution, under extreme circumstances – all efforts should be focused on containing, understanding, recovering from and becoming invulnerable to future occurrences of the cyber risk encountered. In parallel –the organization must continue to deliver its strategic objectives and not let its guard down elsewhere.

Despite numerous surveys and analyses (more or less reliable as the case may be), it is apparent that the human resources of an organization - and those people who have (or can create) legitimate access to its premises, systems and insiders – comprise the most challenging aspect of an organization to secure. Rather than seeing individuals solely as sources of risk, this chapter advances the notion that they can (and should) be seen as a largely untapped security resource.

By extension, the organization(s) and supply-chain(s) which do unleash the protective and responsive potential of their personnel would have significant (and cheap) competitive advantage over others. This cultural re-engineering of values and power is not without its challenges in terms of the courage needed to embrace
The Entrepreneurial Spirit Based on Social Values: The Digital Generation
Innovation and the Entrepreneurship Phenomenon in the Digital Economy (pp. 173-
193).
www.igi-global.com/chapter/the-entrepreneurial-spirit-based-on-social-
values/189817?camid=4v1a

Methodological Issues in the Evaluation of System Analysis and Design
Techniques
www.igi-global.com/chapter/methodological-issues-evaluation-system-
analysis/6127?camid=4v1a