Journal of Management and Business Research, ISSN 2162-8955, *Vol. 1, No. 1, Oct 2011*

Cyberspace Security: How to Develop a Security Strategy

Bel G. Raggad, Ph.D.
Pace University, Pleasantville, NY 10570

Emilio Collar, Ph.D.
Western CT State University, Danbury, CT 06810

Abstract

Despite all of our national borders, varying governments, and security standards, the Internet is effectively removing all connectivity obstacles between countries. People today can more easily connect with anyone around the world. This connectivity, however, comes with a price: our national security. The international community is fully aware of the urgent need to secure the cyberspace. Evidence of this need can be seen in the multiplication of security standards and national schemes interpreting them beyond borders: ISO 15408, ISO 17799, and ISO 27001.

Some countries (including the Security Big Six) are equipped with their security books, policies, and procedures that enable them to feel relatively safe. However, this perceived safety is a false sense of security since these countries continue to share their networks with entities that have less security, or no security at all.

The standards impose security best practices and system specifications for the development of information security management systems. Partners beyond borders have to be secure as this is only possible if all entities connected to the partnership remain secure. Unfortunately, there is no way to verify the continuous security of partners without periodic security auditing and certification, and members who do not comply should be barred from the partnership. This concept also applies to the cyber space or the electronic society [2, 4]. In order to clean our society from cyber crimes and cyber terrorism we need to impose strict security policies and enforce them in a cooperative manner.

The paper discusses the cooperative effort to fight cyber terrorism through 1) strategic alliance, 2) sharing of security plans, and 3) continuous certifications beyond borders. We propose a risk-driven methodology for developing a cooperative security strategy that aims the security of the common cyberspace. All these strategic components are embedded in the development of an auditable ISMS.

Keywords*: Security Audit, Risk, ISO 27001, Certification, ISMS, Security Strategy, Statement of Applicability, Process Approach, PDCA.*