Chapter 6
ICT and Security Governance:
Doing the Right Things the Right Way (and Well Enough)

Eduardo Gelbstein
Webster University, Switzerland

Tom Kellermann
Security Awareness at Core Security, USA

ABSTRACT

To ensure that information systems and data are suitably protected against attacks and malfunctions, good intentions are not enough. Adopting standards and best practices is, by itself, also not enough. The issue is whether things are done well enough to meet the specific requirements of a given environment, be it in national security, manufacturing, electronic commerce, aviation or whatever.

This is not a technical challenge but a governance one. Doing the right things, the right way well enough requires resources (people, money and technology), knowledge, dedication and discipline. Getting all of these together in a sustainable manner is the foundation for success. Failure to do so, is an invitation to disaster.

This chapter examines in summary form those standards and best practices that have been widely accepted as being the "right things the right way" and also discusses how to determine if things are done "well enough".

DOI: 10.4018/978-1-61520-831-9.ch006

1. INTRODUCTION

All that is necessary for evil to triumph is for good men to do nothing. (Edmund Burke (1729 – 1797))

Previous chapters have discussed the critical role of ICT, systems and facilities. The execution of ICT Service Management – the day to day delivery and support – and of ICT Projects is crucial to adding business value and maintaining the security of information assets.

While much of this work is delegated to a Chief Information Officer and a Chief Information Security Officer who use one or more ICT organisations – in house or outsourced – to do this, achieving corporate objectives and complying with legal and regulatory requirements requires more than approving a budget for the ICT function.

The International Standard ISO 38500 published in early 2008 and the initiatives of the Information Technology Governance Institute (ITGI) are the foundation on which this chapter is developed. The purpose of this chapter is to summarize the key components of the governance of ICT and Information Security and list some of the main standards and best practices that have emerged and been widely adopted in the last few years.

Each organization needs to decide what are "the right things", "the right way" and "well enough" in their business context. However, when an ICT organization does not adopt and implement (beyond paying lip service) international standards and proven best practices, it raises questions that executives should examine to ensure their information assets are well managed and protected.

2. THE CONTEXT AND CASE FOR ICT GOVERNANCE

Various sections in this book have touched on the cost and impact of ICT – from service delivery and support to the procurement and development of large systems. These add up to significant numbers.

In 2008 the average cost per employee of service delivery and support was estimated by Gartner Group to be on the order of US $10,000 per year - with around twice this amount in financial services and insurance industries (Smith, Gomolski, Roberts & De Souza, 2008).

Systems procurement and development has a much wider range of costs – from very modest sums to acquire Open Source software such as Apache (for web servers) and Open Office (for basic office tools) to hundreds of millions of dollars for a large Enterprise Resource Planning System (ERP) and beyond. For example, the UK's National Health Service "Connecting for Health" program had, in 2006, a budget for software development of £ 6.2 bn (around US $10 bn), and there are many other projects with development budgets in the billions of dollars.

Not only are these sums significant, but also ICT services or systems are never perfect and, when they are not, there can be a significant impact on the activities of an organization. While the day-to-day activities of executing ICT service delivery and project management are delegated to technical specialists, the items that follow (previously mentioned in Chapter 2) make the case for the active involvement of senior management:

- The cost of downtime

Downtime = the loss of availability, if it extends for a time greater than a certain threshold (which varies from business to business from a few minutes to a day) has several financial components (additional expenditures, lost revenue, liability payments to customers), revenue losses for the duration of the downtime, the loss of customers to competitors as well as a reputational cost if observers are not convinced that the problem was well handled or if such loss of availability happens with unacceptable frequency.

- Cost of lost confidentiality