Chapter 16
Safeguarding Australia from Cyber-Terrorism:
A SCADA Risk Framework

Christopher Beggs
Security Infrastructure Solutions, Australia

Matthew Warren
Deakin University, Australia

ABSTRACT

Terrorist groups are currently using information and communication technologies (ICTs) to orchestrate their conventional attacks. More recently, terrorists have been developing a new form of capability within the cyber-arena to coordinate cyber-based attacks. This chapter identifies that cyber-terrorism capabilities are an integral, imperative, yet under-researched component in establishing, and enhancing cyber-terrorism risk assessment models for SCADA systems. This chapter examines a cyber-terrorism SCADA risk framework that has been adopted and validated by SCADA industry practitioners. The chapter proposes a high level managerial framework, which is designed to measure and protect SCADA systems from the threat of cyber-terrorism within Australia. The findings and results of an industry focus group are presented in support of the developed framework for SCADA industry acceptance.

INTRODUCTION

Cyber-terrorism is "non-state actors' use of ICTs to attack and control critical information systems with political motivation and the intent to cause harm and spread fear to people or at least with the anticipation of changing domestic, national or international events" (Beggs, 2005). For example, an individual who has political motive and penetrates a Supervisory Control and Data Acquisition (SCADA) system controlling gas pressure in a gas plant by manipulating the pipeline and causing an explosion would be classified as cyber-terrorism, because bystanders and civilians would be harmed and motivation to effect political change would have occurred.

SCADA systems have evolved since the 1960s from stand alone systems to networked architectures that communicate across large distances. Their implementation has migrated from custom

DOI: 10.4018/978-1-4666-5942-1.ch016

hardware and software to standard hardware and software platforms (Krutz, 2005). SCADA systems form part of Australia's critical infrastructure. They are used to remotely monitor and control the delivery of essential services and products, such as electricity, gas, water, waste treatment and transport systems (TISN, 2008) The need for security measures within these systems was not anticipated in the early development stages as they were designed to be closed systems and not open systems such as the Internet. The increasingly networked and linked infrastructure of modern SCADA systems has changed those early security plans. Utilities in the industrial control sector have integrated these SCADA networks with their business networks which unfortunately has exposed them to a series of vulnerabilities and risks (Internet Security Systems, 2005).

Currently, organisations within Australia that are controlling critical infrastructure systems such as SCADA are now vulnerable to cyber-terrorism. Attacks and cases in recent years such as the Polish Tram System 2008, Estonia 2007, SQL Slammer 2003, Queensland 2000 and Gazprom 1999, as well as many others, highlight the vulnerability in critical infrastructures and serve to highlight the possibility of cyber-terrorism occurring. These cases and attacks have prompted further research and investigation into the cyber-terrorism threat as research gaps have been recognised by the authors when conducting a literature review on the topic and by interviewing experts in the field. Some of the major gaps identified were the elements of SCADA security risk assessment, terrorist groups' cyber-capability and SCADA critical infrastructure protection including SCADA system vulnerabilities.

For non state actors (Cyber-terrorism group) to be a threat against a SCADA system requires a terrorist or group to have a high level of malicious intent and a high level of knowledge of SCADA systems and ICTs. This paper presents a framework that has been developed to measure and protect SCADA systems from the threat of cyber-terrorism within Australia. The paper also examines the findings and results of a SCADA industry focus group that has been conducted in order to validate the cyber-terrorism SCADA risk framework for industry adoption and acceptance. The framework is made up of the following stages:

CYBER-TERRORISM SCADA RISK ASSESSMENT

This cyber-terrorism SCADA risk assessment subset represents the first stage processes in measuring and protecting SCADA systems from the threat of cyber-terrorism within Australia. The subset discusses the various steps that should be used to conduct a risk assessment on a SCADA system. These steps have been adopted and aligned with the procedures documented in the AS/NZS ISO 31000:2009 risk management standard. Some of the procedures and steps for conducting a risk assessment have been customised to fit a generic SCADA risk assessment and some stages within the process have been modified to suit the SCADA environment. This stage only provides a baseline security risk assessment process that is applicable for SCADA systems. Organisations can use this subset and modify it to suit their SCADA configuration and their organisation requirements and needs.

The purpose of this stage is to provide a generic method for conducting a security risk assessment within a SCADA environment. This subset is the first stage within the cyber-terrorism SCADA risk framework. The subset is based on the AS/NZS ISO 31000:2009 risk management standard which is used by many organisations to conduct risk assessment. This standard has provided the basis for the development of this subset and is referred throughout the document (Based upon Standards Australia, 2009). The cyber-terrorism SCADA risk assessment subset provides the