TISN

FOR CRITICAL INFRASTRUCTURE RESILIENCE

Risk Management for Industrial Control Systems (ICS) And Supervisory Control Systems (SCADA) Information For Senior Executives

(Revised March 2012)

Disclaimer: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

Introduction

This paper provides guidance for Board Members, Chief Executive Officers (CEO), Senior Executives and Risk Managers on the development, the implementation and review of risk management for industrial control systems (ICS) / Supervisory Control and Data Acquisition (SCADA) used in the management and operation of critical infrastructure. Organisations are encouraged to be proactive in assessing and managing risks to these systems and their underlying business processes. Internationally, it is acknowledged that the cyber threat environment is escalating, with targeted attacks having the capability to physically damage infrastructure.

To assist Australian organisations in addressing these risks, Australia's Trusted Information Sharing Network's (www.tisn.gov.au) IT Security Expert Advisory Group (ITSEAG)[1] and its working group, the SCADA CoI,[2] has revised its Generic Risk Management Framework (RMF). The RMF, developed in consultation with owners and operators, is a tool to assist organisations with SCADA systems in assessing their risk exposure and identifying measures to manage risk to an acceptable level.

Why is SCADA risk management important?

It is recognised internationally that, although SCADA systems are reliable, they are highly vulnerable and very difficult to secure.

Senior executives need to have a clear understanding of the threats, vulnerabilities and associated risks to these systems. The challenges facing owners and operators, and the underlying reasons as to why SCADA systems are especially vulnerable, include issues surrounding increased connectivity, interdependencies/supply chains, complexity, continued use of legacy systems and devices and interconnectedness. The Cross-Sector Roadmap for Cyber Security of Control Systems, 30 September, 2011 paper, which was developed by the Industrial Control Systems Joint Working Group (ICSJWG), with facilitation by the US Department of Homeland Security's National Cyber security Division (NCSD) discusses these issues in detail.

The failure or disruption of the day-to-day delivery of essential services to the community could cause a significant loss of brand, organisational reputation and involve judicial action and penalties for non-compliance with regulatory requirements.

[1] The ITSEAG is one of two Expert Advisory Groups established within the Trusted Sharing Information Network (TISN) for Critical Infrastructure Resilience. The ITSEAG provides advice to the Critical Infrastructure Advisory Council (CIAC) and TISN Sector Groups (SGs) on IT security issues as they relate to critical infrastructure resilience. Members of the ITSEAG are information technology/e-security specialists from vendors and consultancy businesses, academic institutions and industry association(s).

[2] The SCADA CoI is an industry-based Working Group of the ITSEAG and a forum for information sharing and collaboration for enhancing the resilience of SCADA systems which support critical infrastructure.

Business drivers for integration with enterprise management systems, has meant that SCADA systems have become interconnected with corporate networks and directly or indirectly with the internet. This high level of integration can extend to remote access by operational staff, suppliers and external organisations, further increasing the exposure of these systems to network vulnerabilities associated with internet threats.

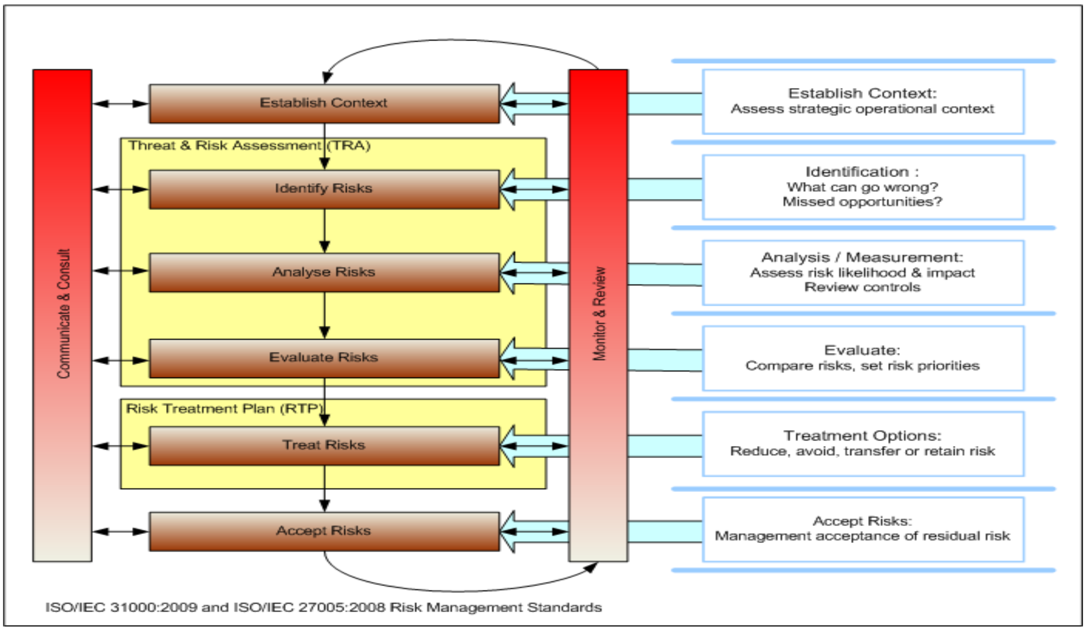
Recent incidents demonstrate that a targeted cyber attack can penetrate traditional corporate cyber defences and cause physical harm to critical infrastructure. Traditional threat sources have evolved and now include nation states, with the threats - such as industrial espionage – becoming more sophisticated and covert.

What is the “Generic SCADA Risk Management Framework”?

The RMF is a high-level document that provides a structured and standards-based approach to identifying and assessing risks for owners and operators of SCADA and industrial control systems. It can be tailored to suit a particular sector or organisation, providing guidance on advice on how information security risks can be simplified and included within existing corporate risk management frameworks.

The RMF utilises national standards such as AS/NZS ISO/IEC31000:2009 Risk Management Principles and Guidelines, ISO/IEC 27005:2011 Information Security Risk Management. As such, it is a tool for Senior Executives and Risk Managers to use to determine risk exposures for their enterprise, using a common language and terminology.

The figure summarises the risk management process applied throughout the RMF.



ISO/IEC 31000:2009 and ISO/IEC 27005:2008 Risk Management Standards

The scope of the Generic SCADA Risk Management Framework

Business planning includes management strategies for financial, competitive, strategic, global, reputation and legal and community risks. These arrangements may omit other risk categories such as people, management and control measures, information management, communication and computer network connectivity, SCADA software, hardware and field devices and interdependencies such as power/energy and water suppliers. These are also essential to the development of risk mitigation and the ongoing functioning of a business.

The Framework provides broad guidance to owners and operators of SCADA systems for managing their risks and designed to be adaptable to the need of the different industry sectors. Use of the Framework by industry will contribute to improving the security of national critical infrastructure, with the potential of reducing costs. It identifies common enterprise level individual risk factors through a validated 'Threat and Risk Assessment' and outlines a generic 'Risk Treatment Plan' for mitigating identified risks.

What is the advantage of this 'Framework' and a common approach?

The RMF is generic and, as such, is designed to be a useful tool for all owners and operators of critical infrastructure to utilise. The RMF clearly identifies consequences and major stakeholders responsible for common points of failure, whether they are malicious, accidental, natural or environmental to ensure the confidentiality, integrity and the availability of SCADA ICT systems and information they contain.

These factors are stated in plain language and in such a way that Boards, CEOs and Senior Executives and technical and operational personnel can agree on documentation, decisions and actions for their SCADA and industrial control systems that are:

- standards based best practice;
- consistent with governance for:
    - corporate policies and practices, and
    - regulatory compliance, and
- cost effective.

What questions can you ask?

Board Members, CEOs, Senior Executives and Risk Managers should seek answers from Chief Information Officers (CIO), Chief Information Security Officers (CISO) and Engineering Managers to the following questions:

- Do we have a standards-based approach to managing enterprise risks associated with our SCADA systems?
- Do our overall enterprise security policies and practices include SCADA and other industrial control systems as part of the holistic approach to managing enterprise vulnerabilities to communications, IT and other security risks?
- Is there appropriate 'top down' management for effective control and management of enterprise SCADA and industrial control systems within our security framework?

- Do our security policies and practices take into account how our corporate IT and SCADA and industrial control systems, and our physical and personal security policies and practices overlap?
- Do we monitor all our corporate security and privacy practices for regulatory compliance and industry good practice?
- How often does our organisation undertake vulnerability assessments of key business processes and supporting IT infrastructure?
- Do our IT security incident/emergency management processes include SCADA specific handling and escalation process/procedures?

Summary

Risk management is a strategic element of a company's ongoing business planning. Good governance and regulatory compliance requires that Board Members, CEOs, Senior Executives and Risk Managers mitigate risks for these functions and the supporting ICT, ICS and SCADA systems.

SCADA and industrial control systems along with the communication networks they use are the central nervous system for a vast array of sensors, alarms and switches that provide automated control and monitoring for these functions. These functions and systems are increasingly vulnerable to potential harm and require protection from malevolent cyber attack or accidents.

The RMF contains specific risk management guidance for Executives, Risk Managers, CIOs and CISOs and is available from www.tisn.gov.au.

For Further Information

The Department of Broadband Communications and the Digital Economy provides Secretariat support to both the ITSEAG and the SCADA CoI. Enquiries regarding these groups and/or for more information on the SCADA Generic Risk Management Framework can be made by telephoning 02 6271 1595 or emailing itseag@dbcde.gov.au or scada@dbcde.gov.au.

****