Chapter 14

Information Sharing for CIP: Between Policy, Theory, and Practice

Neil Robinson
RAND Europe, UK

ABSTRACT

This chapter describes and contrasts policy, economic theory, and insights concerning the establishment and operation of Information Exchanges (IE). In the context of this chapter, IEs are specific mechanisms meant to stimulate the exchange and sharing (aside from pure disclosure) of a range of confidential information relating to security between owner-operators of critical infrastructure. Information shared in IEs may be of varying types but is reported to generally be of a non-technical nature. In the Supervisory Control and Data Acquisition (SCADA) community, a number of nations have established IEs; for example, European SCADA and control systems exchange has been operating since 2005. The chapter primarily considers these issues through the perspective of efforts to address the security of the Critical Information Infrastructures (CII). Despite IEs being seen by policy-makers as important to tackle CIP issues, limited empirical operational evidence exists to suggest that IEs constitute a useful mechanism to successfully overcome the economic incentives governing the disclosure of information. The chapter concludes by identifying opportunities to further explore the disparities and reasons for the indicative disjuncture between economic theory, policy, and practice. The chapter is thus aimed primarily at managers, policy-makers, and non-technical personnel considering participation in an IE.

INTRODUCTION

The vulnerability of critical infrastructures to various types of physical and cyber incidents remains high on the policy agenda, especially after the headlines generated by the appearance of Stuxnet (Bellovin; 2010). There is increasing interest in the security of critical infrastructures, driven by a number of related developments.

Firstly, margins of profit for infrastructure operators in the increasingly globalised economy have led to those firms owning or operating criti-
cal infrastructures to seek more and more ways to cut costs, often at the expense of security. This, in conjunction with the now pervasive presence of the Internet in all walks of life, has resulted in firms owning or operating critical infrastructure evaluating the use of public networks as a route to deploying some aspects of their control systems.

Secondly, the increasing confluence of connectivity between operational systems that link to PCS with business information systems (used for billing, revenue management and other back office operations) has meant that the potential for damage increases significantly (Riptech; 2001). It is received wisdom that attack dynamics are changing. Although extensive research into those that developed Stuxnet indicated that this took a team of 4-6 people server months to prepare, the increasing proliferation of easy to use, accessible tools on the criminal underground also drives the increased risk to Critical Infrastructures. Concern over the increasing use of Commercial Off the Shelf Technology (COTS) and the connection of SCADA systems to other potentially more insecure networks would appear to be supported by recent evidence concerning the expectations of infrastructure owner operators to link up elements of their infrastructure:

*The key observation to report again this year is that links from/to control center-based systems are substantial, and indeed appear to be continuing to increase from what was once a completely closed control center-based system. (Newton-Evans, Market Trends Digest, 2008, p4)*

Thirdly, and perhaps most importantly for the subject of this chapter, unlike historical consideration of infrastructure risk, it is widely regarded that the majority of such infrastructure is owned and or operated by the private sector (Assaf; 2008) although there has been criticism of the provenance of specific percentages used as received wisdom (Bellavita; 2009). Nonetheless, the need to obtain private sector involvement in securing these networks has been noted in various forms of declaratory policy including for example the US White House 60 day Cybersecurity Policy Review. This concluded that the private sector “designs, builds, owns and operates most of the network infrastructures that support government and private users alike” (White House; 2009).

Technical estimations of the threat and risk posed to these infrastructures vary. For example, following disclosure of news of a specific vulnerability, security expert Bruce Schneier indicated that vulnerabilities in SCADA security were an important concern (Schneier; 2007). Shapiro et al (2011) conducted an assessment of the vulnerability of SCADA devices whilst in Rosslin and Choi (2009) the vulnerabilities of SCADA control systems are further explored. Security researchers and experts agree that conceptions concerning the standalone nature of SCADA systems, the high security applied to such systems and the bespoke character of software used to run SCADA are largely false (Rosslin and Choi; 2009 and Riptech; 2001).

Nonetheless, the private sector faces a dilemma in addressing cyber-security with respect to these contextual factors, namely that they must understand how a wide range of imperatives (especially financial) drive security and the possibilities to mitigate security risks in an increasingly diverse operational environment. These financial drivers interact with other pressures that add to the complexity of making security investment decisions. For owner-operators of Critical Infrastructure, one of the main factors stems from government, who may be concerned that the security of infrastructure whose failure might have serious national implications, is put at risk by the private sector ignoring security. Although the concerns relating to regulation apply to those strategically important owner-operators of Critical Infrastructure, the complexity of applying security cost benefit trade-offs applies more broadly to a range of security issues.
Related Content

End-to-End (E2E) Security Approach in WiMAX: A Security Technical Overview for Corporate Multimedia Applications
[www.igi-global.com/chapter/end-end-e2e-security-approach/22082?camid=4v1a](www.igi-global.com/chapter/end-end-e2e-security-approach/22082?camid=4v1a)

A Quantum Secure Entity Authentication Protocol Design for Network Security
[www.igi-global.com/article/a-quantum-secure-entity-authentication-protocol-design-for-network-security/237207?camid=4v1a](www.igi-global.com/article/a-quantum-secure-entity-authentication-protocol-design-for-network-security/237207?camid=4v1a)

An Efficient, Anonymous and Unlinkable Incentives Scheme
[www.igi-global.com/article/an-efficient-anonymous-and-unlinkable-incentives-scheme/148300?camid=4v1a](www.igi-global.com/article/an-efficient-anonymous-and-unlinkable-incentives-scheme/148300?camid=4v1a)

Challenges and Solutions for DNS Security in IPv6
[www.igi-global.com/chapter/challenges-and-solutions-for-dns-security-in-ipv6/78870?camid=4v1a](www.igi-global.com/chapter/challenges-and-solutions-for-dns-security-in-ipv6/78870?camid=4v1a)