Adoption of ISMS for Protecting SCADA Systems against Cyber Terrorism Threats

Zahri Yunos, Nor'azuwa Muhamad Pahri, Mohd Shamir Hashim, Rahayu Ahmad
CyberSecurity Malaysia
Seri Kembangan, Malaysia
Email: Zahri {at} cybersecurity.my

Abstract—**The potential for catastrophic cyber attacks that can cripple the operations of critical infrastructures of nations is worrying. The consequences of cyber attack to the Supervisory Control and Data Acquisition (SCADA) systems are wide, resulting in potentially catastrophic damages and disruption. This paper proposes for the Critical National Information Infrastructure (CNII) organizations to comply with the ISO/IEC 27001:2013 or Information Security Management System (ISMS), which provides a systematic guidance for the organization's information security risks management and the implementation of security controls to reduce such risks to an acceptable level. The implementation of the ISMS certification in Malaysia's CNII will be the case study of this paper. Future works in this area can be further conducted, which may lead to the development of critical infrastructure protection (CIP) programs and the development of risk management frameworks to counter threats from cyber terrorism attacks for CNII.**

Keywords- Critical National Information Infrastructure (CNII); Cyber Terrorism; Cyberspace; SCADA

I. INTRODUCTION

In this digital age, the concept of cyber terrorism or the use of cyberspace to carry out terrorist activities has emerged. Many stakeholders are concerned with terrorists' attacks against their critical infrastructures such as the telecommunications and power distribution networks, transportation systems, and essential public utility services [1], [2]. Cyber terrorism can be seen as a relevant threat due to its strong relation with ICT and the cyberspace.

The CNII underlies the nation's economic, political, strategic and socio-economic activities [3], [4]. These sectors such as energy, transportation and information & communications, now rely heavily on ICT systems to manage daily operations through Control Systems such as SCADA and Distributed Control Systems (DCS). These critical systems require national protection against cyber threats.

II. LITERATURE REVIEW

A. *Understanding Cyber Terrorism*

Terrorism nowadays may be targeted at computer systems that control a nation's critical infrastructure services. Denning [5] defines cyber terrorism as unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Mantel [6] defines cyber terrorism as highly damaging computer attacks by private individuals designed to generate terror and fear to achieve political or social goals. Cyber terrorism involves computer technology use as a weapon or target by terrorist groups or agents [7].

Based on the discussions above, simple definition of cyber terrorism is the use of ICT and its means by terrorist groups and agents to promote extremist or aggressive tendencies, usually politically motivated which lead to forceful or catastrophic impact [8], [9], [10], [11]. The perpetrator must use information systems or other electronic means to launch cyber attack against CNII. The definition above also suggested that serious attacks against CNII could be acts of cyber terrorism.

B. *Threats to the SCADA Systems*

The Critical infrastructure organizations have been using the SCADA system for gathering real time data, controlling processes and monitoring equipment from remote locations [12]. The SCADA systems are used to monitor and control the delivery of critical services such as power, waste treatment, nuclear power generation, transportation and water supply. Previously, the SCADA systems are closed operating environment (or stand alone systems), however with the advancement of the internet and the need for connectivity, the trend for these systems is towards open standards (or networked architecture). This could be the Ethernet, TCP/IP or web technologies where vulnerabilities are widely known [13]. The trend of terrorist groups using the cyberspace for their activities is leading to potential cyber attacks against a country's critical infrastructure ICT network and SCADA systems.

There is an increasing risk to CNII sectors that rely on these systems that can be damaged or disrupted by intentional cyber attacks. Such incidents could potentially have a significant and potentially overwhelming impact on the national economy, security and public safety. There were many scenario of cyber incidents occurring to these sectors such as the cyber attack that have caused at least one power outage affecting multiple cities outside the United States [14], installation of unauthorized software and damaging the computer used to divert water from the Sacramento River [15], the Brazil blackout in year 2005 and 2007 [16], the cyber attacks on US oil industry [17], the Seven Jersey City Heights water mains break [18] and the Stuxnet worm/Trojan attack [19].

It is also known that the use of off-the-shelf IT systems for SCADA systems is common. The servers and field devices may use Ethernet and TCP/IP as the network protocol, with software and Operating Systems that are widely used by business systems for easier connections between various systems resulting in lower operating and maintenance cost. However, this introduces the control systems to the same cyber security risk faced by the business network, thus a higher risk from cyber threats [20]. The interest in SCADA networks from the hacker community is rising due to the destruction it can cause to the operation of CNII when disrupted.

III. Security Requirements For SCADA Systems

It is important to know security requirements or measures for ensuring protection of the SCADA systems from cyber attacks. It is often argued that SCADA system security is special and different from the traditional information security or information technology security. This is because of the environment that the SCADA systems are used within, and the requirements placed on them.

Stouffer et.al [21] highlighted that the SCADA systems need cyber security operational strategies. Therefore, they recommended security countermeasures to mitigate the associated risks. Due to the many different levels of SCADA systems, they encouraged to perform a risk-based assessment on the systems and to tailor the recommended guidelines and solutions to meet the specific security, business and operational requirements. Stouffer et al. [21] suggested that securing an ICS is based on a combination of effective security policies and properly configured set of security controls that consist of management, technical and operational controls.

Likewise, Kiuchi and Serizawa [20] argued that security requirements may need to be tailored to each SCADA system. There are many emerging security technologies applicable to this system and many security standards and guidelines are being adapted to control systems, which can be a guide when selecting the appropriate and sustainable security requirement.

IV. Case Study: Adoption of ISMS in Malaysia's CNII

The National Cyber Security Policy of Malaysia is a holistic approach in providing cyber security to the country's CNII. It has outline eight (8) areas of focus called thrusts covering all aspect of cyber security (Table 1). Under Cyber Security Technology Framework (PT3), one of the outlined action plans is to have information security standards be implemented in the CNII organizations for certification.

TABLE I. National Cyber Security Policy of Malaysia

Policy Thrust (PT)	Policy Thrust Focus Area
PT1	Effective Governance
PT2	Legislative and Regulatory Framework
PT3	Cyber Security Technology Framework
PT4	Culture of Security and Capacity Building
PT5	Research and Development Towards Self-Reliance
PT6	Compliance and Enforcement
PT7	Cyber Security Emergency Readiness
PT8	International Cooperation

CNII organizations that use SCADA system can be protected from physical or cyber threats by implementing the ISO/IEC 27001:2013 Standard or ISMS in their respective organizations. This Standard systematically examines the organization's information security risk and implement security controls to reduce such risks to an acceptable level. By implementing ISMS, attention can be focused on mitigating risks, defining protective security measures and selecting control for mitigation strategies of all threats. The ISMS also requires stakeholders and management commitment to ensure successful implementation of the standard in the organization.

The proposal for Malaysia's CNII to be ISO27001:2013 certified was tabled at the Cabinet Minister Meeting in year 2010. The proposal was accepted and the country's CNII were given two (2) years to obtain ISMS certification. The National Security Council, through the sector leads of the 10 CNII sectors, identified about 200 CNII organizations and CyberSecurity Malaysia assisted in providing the plan for the certification implementation.

The implementation program was divided into 3 main phases:

Phase 1: Awareness – The relevant organizations were to identify teams of officers that responsible in implementing ISMS within the organization. A schedule was developed to instill awareness to these teams. Assistance was provided to identify the critical area within their respective organization for certification in line with the requirement of the policy in CNII protection. A few awareness sessions was done and the team utilized these sessions to seek further clarification on the ISMS, their term of references as implementers and exchanging concerns with each other.

The CNIIs are recommended to implement the necessary security controls in compliance with the ISMS. The Standard certification is one of the most used corporate best practices for ICT security standards, addressing management requirements

as well as identifying specific control areas for information security. It provides a comprehensive framework for designing and implementing a risk-based Information Security Management System. The requirements and guidance cover policies and actions that are necessary across the whole range of information security vulnerabilities and threats.

Phase 2: Training – Following the awareness phase, the teams attended several training sessions on ISMS. CyberSecurity Malaysia and the Malaysian Administrative Modernization and Management Planning Unit (MAMPU) provide the necessary module to the team to identify area of certification, setting up the necessary work processes and implementation of the Standard.

Phase 3: Audit – The final phase is teaching the teams to audit the implementation of the ISMS in their respective organization. These sessions focus on the progress of the implementation and area of improvement that can be done. In these sessions, the teams provide feedbacks on implementation issues and together with other team and the facilitator discuss on the best way forward to overcome those issues.

ISMS has been used by the critical sectors as the baselines reference and comparison in determining the security requirements for SCADA systems. Although this standard is not focused on SCADA systems, it is commonly used security standard in the electric utility industry [22]. The methods from this standard are efficiently use for security management in electric utilities as well as for security assessments of power distribution operations [23].

ISMS is intended to bring formal specification of information security under explicit management control. It is a mandated specific requirement, where organizations can therefore be formally audited and certified compliant with the standard.

V. CONCLUSION

CNII organizations have been using the SCADA system to monitor and control the delivery of critical services. Such services are crucial to the nation because the destruction or disruption of these services would significantly affect the economic strength, image, defense and security, government capabilities to function, and public health and safety. The potential for catastrophic terrorist cyber attacks that cripple critical infrastructure is imminent.

This paper recommends the implementation of ISO/IEC 27002:2013 Standard or ISMS to measure and protect SCADA systems from cyber terrorism threats and provided a case study of the Standard implementation in Malaysia. The implementation provided great significance and value in protecting organization assets against cyber terrorism.

Malaysia has aggressively pursued the adoption and certification of ISO 27001:2013 Standard or ISMS within the CNII organizations. Within the 2 years given, more than 70% of these organizations have been ISMS certified.

For future works, there are possible areas that can be further conducted,

a) Development of Critical Information Protection Programs in combating cyber terrorism. This will provide extra advantage to policy makers and stakeholders to develop better strategy and policy framework against such threats.

b) Development of risk management framework to measure and protect SCADA systems from the threat of cyber terrorism in Malaysia. This reduces the risk of cyber attack and its impact to CNII, thus providing readiness against cyber terrorism. The risk management framework assists in predicting what can happen and the possible consequences, and recommends remedial action to reduce risk to an acceptable level.

REFERENCES

[1] R. Ahmad, Z. Yunos, S. Sahib, and M. Yusoff, "Perception on Cyber Terrorism: A Focus Group Discussion Approach," *J. Inf. Secur.*, vol. 03, no. 03, pp. 231–237, 2012.
[2] I. Bernik and K. Prislan, "Cyber Terrorism in Slovenia - Fact of Fiction," in *The 3rd International Multi-Conference on Complexity, Information and Cybernatics*, 2012.
[3] J. Russell and R. Cohn, *Critical Infrastructure Protection*. Bookvika Publishing, 2012, p. 5.
[4] Z. Yunos, R. Ahmad, S. M. Ali, and S. Shamsuddin, "Illicit Activities and Terrorism in Cyberspace : An Exploratory Study in the Southeast Asian Region," in *Pacific Asia Workshop on Intelligence and Security Informatics (PAISI 2012), Malaysia, 29 May, Springer Lecture Notes in Computer Science, Volume 7299/2012*, 2012, pp. 27–35.
[5] D. E. Denning, "A View of Cyberterrorism Five Years Later," in *Internet Security: Hacking, Counterhacking, and Society*, K. Himma, Ed. Jones and Bartlett Publishers, 2007, p. Chapter 7.
[6] B. Mantel, "Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?," *CQ Res.*, pp. 129–152, 2009.
[7] M. Conway, "What is Cyberterrorism and How Real is the Threat? A Review of the Academic Literature, 1996-2009," in *Law, Policy, and Technology - Cyberterrorism, Information Warfare, and Internet Immobilization*, P. C. Reich and E. Gelbstein, Eds. Hersey, PA: Information Science Reference, 2012, p. 279307.
[8] R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," *Int. J. Comput. Sci. Inf. Secur.*, vol. 10, no. 2, pp. 149–158, 2012.
[9] R. Ahmad, Z. Yunos, and S. Sahib, "Understanding Cyber Terrorism : The Grounded Theory Method Applied," in *IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic, Malaysia, 26-28 June*, 2012, pp. 334–339.
[10] Z. Yunos, R. Ahmad, and N. A. A. Abd Aziz, "Definition and Framework of Cyber Terrorism," *Proceeding Southeast Asia Reg. Cent. Count. Terror. Sel. Artic.*, vol. 1/2013, pp. 67–79, 2013.
[11] Z. Yunos and R. Ahmad, "The Application of Qualitative Method in Developing a Cyber Terrorism Framework," in *Proceedings of the 2014 International Conference on Economics, Management and Development (EMD 2014)*, 2014, pp. 133–137.
[12] R. Lemos, "System Makers Pushed Toward Security," 2011, vol. 2.
[13] C. Beggs, "Cyber-Terrorism in Australia," *IGI Glob.*, pp. 108–113, 2008.
[14] T. Claburn, "CIA Admits Cyberattacks Blackout Cities," 2008. [Online]. Available: http://www.informationweek.com/news/205901631. [Accessed: 05-Oct-2011].
[15] R. McMillan, "Insider Charged With Hacking California Canal System," 2007. [Online]. Available: http://www.computerworld.com/s/article/9050098/ Insider_charged_with_hacking_California_canal_system. [Accessed: 05-Oct-2011].
[16] Physorg.com, "Brazil Blackouts Result of Cyber Hacking." 2009.
[17] M. Clayton, "US Oil Industry Hit By Cyberattacks: Was China Involved?" 2010.
[18] M. Conte and D. . Gibson, "Seven Jersey City Heights Water Mains Break Due To Computer Glitch." 2009.

[19] N. Falliere, L. . Murchu, and E. Chien, "W32.Stuxnet Dossier." 2011.
[20] M. Kiuchi and Y. Serizawa, "Security Technologies, Usage and Guidelines in SCADA System Networks," in *ICROS-SICE International Joint Conference 2009, Fukuoka International Congress Center, Japan*, 2009.
[21] K. Stouffer, J. Falco, and K. Kent, "National Institute of Standards and Technology: Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security." Recommendations of the National Institute of Standards and Technology, Special Publication 800-82, Final Public Draft, 2008.
[22] T. Sommestad, G. . Ericsson, and J. Nordlander, "SCADA System Cyber Security – A Comparison of Standards." Power and Energy Society General Meeting, 2010 IEEE, 2010.
[23] L. Nordstrom, "Assessment of Information Security Levels in Power Communication Systems Using Evidential Reasoning," *IEEE Trans. Power Deliv.*, vol. 23, no. 3, pp. 1384–1391, 2008.