Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2009

Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption

Christopher Beggs
Monash University

Matthew Warren
Deakin University

Originally published in the Proceedings of the 10th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st-3rd December, 2009
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/5

Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption

Christopher Beggs[1] and Matthew Warren[2]
[1]Faculty of Information Technology
Monash University, Australia and Sinclair Knight Merz

[2]School of Information Systems
Deakin University, Australia

Abstract

Terrorist groups are currently using information and communication technologies (ICTs) to orchestrate their conventional physical attacks. More recently, terrorists have been developing a new form of capability within the cyber-arena to coordinate cyber-based attacks. This paper 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 paper is an extension of work previously published by Beggs and Warren 2008, it presents a high level overview of a cyber-terrorism SCADA risk framework that has been adopted and validated by SCADA industry practitioners. The paper proposes a 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 adoption and acceptance.

Keywords

Cyber-terrorism, cyber-capability, SCADA, critical infrastructure.

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 hardware and software to standard hardware and software platforms (Krutz, 2006). 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, (See Appendix for descriptions) 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.

CYBER-TERRORISM SCADA RISK FRAMEWORK

A cyber-terrorism SCADA risk framework was developed and adopted to suit a SCADA environment. The framework involves a three stage process which organisations need to follow to measure and protect SCADA systems from the threat of cyber-terrorism. The results and findings of a SCADA industry focus group is presented later in support of the frameworks worthiness, acceptance and adoption within an industry based context.

The process for organisations involves three stages which are listed below:

- Stage 1- AS/NZS 4360: Cyber-terrorism SCADA Risk Assessment-(Subset);
- Stage 2- Cyber-terrorism SCADA Capability Assessment Model;
- Stage 3- AS/NZS 27002:2006 Cyber-terrorism-SCADA Controls-(Subset).

The paper will describe the key stages of the framework.

STAGE 1 AS/NZS 4360:2004 CYBER-TERRORISM SCADA RISK ASSESSMENT SUBSET

The cyber-terrorism SCADA risk assessment subset represents the first stage process in measuring and protecting SCADA systems from the threat of cyber-terrorism within Australia. The subset has been adopted for a SCADA environment and discusses the various steps that should be used to conduct a risk assessment on a SCADA system. These steps have been derived and aligned with the procedures documented in the AS/NZS 4360:2004 risk management standard (Based upon Standards Australia, 2004). 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 subset only provides a baseline (high-level) 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 *(See Beggs and Warren 2008 for further details of stage 1).*

The key areas that are mentioned in this subset are the main elements of the risk management processes for a SCADA system which include:

- Communicate and consult SCADA;
- Establish the context for SCADA;
- Identify risks of SCADA;
- Analyse risks of SCADA;
- Evaluate risks of SCADA;
- Treat risks for SCADA;
- Monitor and review SCADA.

(Based upon Standards Australia, 2004)

STAGE 2 OF CYBER-TERRORISM SCADA RISK FRAMEWORK: CYBER-TERRORISM SCADA CAPABILITY ASSESSMENT MODEL

The second stage of the cyber-terrorism SCADA risk framework is the cyber-terrorism SCADA capability assessment model. This assessment model examines and analyses the level and identifies the indicators of cyber-capability terrorist groups need to acquire to orchestrate cyber-terrorism. The assessment model consists of a cyber-terrorism SCADA capability model which demonstrates eight indicator levels of cyber-capability a group would

require to carry out a cyber-terrorist attack against SCADA systems within Australia. This capability model can be used by organisations as a tool to measure the level of cyber-capability terrorist groups possess. The assessment model consists of guidelines and procedures on how to use the capability model and provides organisations with a tool to measure terrorist group's cyber-capability to orchestrate cyber-terrorism. These tools are described in Table 1 and Table 2.

The model which has been developed by the present authors should be used as the second major step in measuring and protecting SCADA systems from the threat of cyber-terrorism within Australia.

Table 1. Terrorist Motive to Orchestrate Cyber-terrorism-Validated

Terrorist Motive Required for a Cyber-terrorist Attack in Australia	**Indicator**
Political/Motivation- For an individual terrorist or group to orchestrate a cyber-terrorist attack against Australia they initially would need to have acquired a very high level (e.g. equivalent score of 5) of anti-Australian sentiment with political motivation to spread their ideology or to generate change by creating fear through an attack using or targeting ICT.	Yes/No

Table 2. Cyber-terrorism SCADA Capability Model- Validated

Terrorist Cyber-Capability Level Indicators Required for a Cyber-terrorist Attack in Australia	**Score Range**
Terrorist leaders and members with advanced ICT skill set- This level capability indicator requires terrorist leaders to have advanced knowledge of ICT including: TCP/IP, advanced cryptography, Botnets, Biometrics, and other associated security technologies.	1-5
Terrorists with advanced hacking tools and techniques- This capability level indicator would require education in ICTs and software training e.g. hacking tools and hardware to orchestrate an attack.	1-5
Access to new advanced ICTs- This capability level indicator involves terrorists or groups having access to new emerging technologies. E.g. biometrics, advanced encryption.	1-5
Advanced knowledge of SCADA systems- This capability level indicator involves terrorists having a high level of SCADA knowledge including; software engineering, middleware, application layer and backend.	1-5
Terrorist insiders within the organisation of selected target- this capability level indicator involves having a terrorist or member inside a critical infrastructure organisation such as power, gas, water etc, either within their IT department or operational control department.	1-5
Reconnaissance- this capability level indicator requires scanning and probing SCADA networks to find and detect SCADA vulnerabilities in order to prepare for attack.	1-5
Funding- this capability level indicator requires financial backing within the group to orchestrate attacks. This includes equipment, training, hiring, planning, organising, educating, etc.	1-5
Total Level of Cyber-Capability Indicators	Score =7-35

CAPABILITY MODEL METHODOLOGY AND GUIDELINES FOR ORGANISATIONS

The proposed model has been developed and is based on supporting literature and case studies such as Queensland 2000, SQL Slammer 2003, and Gazprom 1999 (See Appendix for case details). The model is a guide for measuring a terrorist group's cyber-capability for coordinating a cyber-terrorist attack against SCADA systems within Australia. Currently, there is no evidence of a cyber-terrorist attack being recorded or occurring within the Australian context or overseas. Consequently, it is difficult to predict the capability required for such an attack.

It would only be possible to determine whether a terrorist group possesses advanced SCADA capability or advanced hacking techniques if it has previously demonstrated its cyber-capabilities in some way. Hence senior security managers may have to make some evaluations of cyber-capabilities based on how other terrorist groups, hackers and extremist groups have used ICT. Therefore, while the model includes hypothetical elements, it is grounded in concrete examples of how anti-social elements have used ICTs to advance their agendas or to cause destruction, including instances of harming individuals or attacking critical infrastructures.

For instance, if a terrorist group such as Al-Qaeda has demonstrated all capability levels, then its cyber-terrorism SCADA capability level would be very high and the possibility that it could conduct a cyber attack would be more likely. Therefore, the model presents a foundation to measure and to estimate the cyber-capability of terrorist groups depending on the available information at hand.

The model consists of eight indicator levels of cyber-capability to orchestrate a cyber-terrorist attack. The first level indicator political motivation must be either non-mandatory or mandatory with either a Yes/No as the political motivation capability level must automatically receive a score of 5 (very high) for it to be classified as an act of terrorism in order to start the cyber-terrorism lifecycle. All other seven capability levels are equally important and are mutually exclusive. Therefore they have same weighting and importance. For a terrorist group to have the maximum chance of orchestrating an attack, all cyber-capability level indicators need to be obtained with the highest scores possible 35/35. For example, if a group's capability only involves four out of the eight capability levels with medium scores of 3 in each capability level (16/35), then a group's likelihood of such an attack would be minimal. However, the more capability levels that are obtained will ultimately increase the likelihood of the group having the ability to orchestrate an attack. Another example could consist of a terrorist group obtaining six out of the eight capability levels with very high (5) scores e.g. 30/35. Although all levels have not been obtained, their chances would be increased. It is important to acknowledge that all capability level indicators should be valued equally since defining and measuring the relative importance of each capability level indicator is not quantifiable. For example, if a terrorist group has advanced knowledge of SCADA, but minimal knowledge of hacking, then penetrating a SCADA system would be near impossible. Similarly, if a terrorist group acquired advanced hacking techniques but had limited funding (e.g. laptops, software, training, planning, organising) then successfully orchestrating an attack would be also difficult. This suggests that it is not a viable option to evaluate and measure which capability level is more important than another and recommends that all capability levels have an important role in orchestrating a cyber-terrorist attack.

Examples of Cyber-terrorism Capability Scores

One of the issues relating to terrorist groups is that they have varying capabilities. The variability is described by Table 3, this shows the score range for each capability level. This score range indicated below is an example of how the cyber-terrorism SCADA capability model could be used by an organisation. This score has been derived based on a sample range of 1-5 but could be flexible and adaptable to change depending on the organisations needs and requirements.

Table 3. Cyber-terrorism Scoring Matrix

Score	Range	Description
1	Very Low	Terrorist group has developed or acquired very low capability if any;
2	Low	Terrorist group has developed or acquired a low level of capability;
3	Medium	Terrorist group has developed or acquired a medium level of capability;
4	High	Terrorist group has developed or acquired and demonstrated a high level of capability;

5	Very High	Terrorist group has developed or acquired and demonstrated a very high level of capability.

GUIDELINES AND PROCEDURES FOR ORGANISATIONS

Organisations should use external cyber-terrorism experts in this stage of the framework to assist in the examination of terrorist groups' cyber-capability to orchestrate a cyber-terrorist attack against their organisation and Australia. These experts should be outsourced from specialised security agencies, both government and private and should form the basis of a cyber-terrorism steering group who will have the knowledge and expertise on terrorist groups and their cyber-capabilities. The use of experts from trusted agencies such as ASIO, Defence Signal Directorate, TISN, Attorney Generals Department, Defence Department, Universities and other associated agencies would enable a wide range of experts to assist with estimating and assessing scores increasing the validity of the scores.

The capability model requires cyber-terrorism experts to analyse the different indicator levels of capability required to orchestrate a cyber-terrorist attack. Organisations should seek advice from these experts in regards to their risk category and threat level of a cyber-terrorist attack against SCADA systems within Australia. Organisations should review these capability indicator levels regularly by appointing the necessary cyber-terrorism expertise from chosen security professionals or security agencies. For example, organisations should create communication channels with security professionals and agencies to develop a group of experts who can make an assessment on the capability and the threat of terrorist groups. Professionals or agencies could be developed from agencies discussed above.

Cyber-terrorism experts should apply their expertise and knowledge of a terrorist group's cyber-capability indicator levels to evaluate the cyber-terrorism SCADA capability model. This can be achieved by completing a cyber-terrorism capability questionnaire for example which provides methods for data gathering to evaluate the level of cyber-capability terrorist groups possess (which is beyond the scope of this paper). Once the questionnaire is completed, organisations can assess a terrorist group's cyber-capability levels by analysing the results from all the experts who have participated in the survey. The results should be analysed by taking the average mean of all experts' opinions and responses. These results can than determine the level of cyber-capability terrorist group's posses and can be used to evaluate the likelihood of a cyber-terrorist attack against SCADA systems within Australia. This suggests that the example of a questionnaire only provides a basis for making an assessment and other methods could be developed by the cyber-terrorism steering group depending on the needs and requirements of the organisation. For example, using previous cases and literature could be a possible method that organisations adopt in order to make an assessment for the cyber-terrorism SCADA capability model.

Cyber-terrorism SCADA Capability Model Applied To Queensland Case 2000

The cyber-terrorism SCADA capability model could also be applied to previous cases such as the Queensland case 2000 (See Appendix). Although this case is not classified as cyber-terrorism by strict definition, this case is closely related and can also demonstrate how the cyber-terrorism SCADA capability model could be used to determine other threats to critical infrastructure and ICT. The case and cyber-capability indicators have been broken down and analysed by the present authors with discussion below:

- *Political Motivation*: there was very low political motivation (if any) and intent for the employee to spread their ideology or to generate change by creating fear through an attack using or targeting ICT. The case

presented minimal signs of political motivation as the attacker was just a disgruntled employee seeking revenge about being refuted a job position;

- *Advanced ICT Skill Set*: a high level of ICT skill set was demonstrated by the attacker such as TCP/IP connections and bypassing security related technologies even if they were present which is restricted information and unknown.
- *Hacking tools and Techniques*: was highly demonstrated in this case as he had full control of the SCADA systems and was able to release raw sewerage over a 4 month period. The hacker was directly connecting into the system as a mobile pump station (142 Sewage Pumps, 2 monitoring Computers and 3 Radio Frequencies). Security mechanisms were not properly in place for remote access and the SCADA network was not configured properly with firewall protection between SCADA the network and the corporate network. Also the laptop found had evidence of other hacking attempts
- *Advanced Knowledge of SCADA*: the attacker had a very high level knowledge of SCADA systems as he was already working for Hunter WaterTech prior to the incident as a SCADA consultant;
- *Insider*: the attacker was an insider of Hunter WaterTech a client of Maroochydore Water Services and was able to use information as well as a laptop from Hunter WaterTech to orchestrate his attacks against Maroochydore Water Services. This suggests that the attacker was a very high level insider between both organisations, who had the ability to carry out such an attack as he had previous knowledge and insight of the sewerage system;
- *Reconnaissance*: this was most likely very low as he already had knowledge of the current system through Hunter WaterTech so scanning SCADA networks may have been unnecessary or limited in this case.
- *Funding*: this was low because he had already stolen the software and the laptop from Hunter WaterTech. So there was no real need for funding in terms of equipment, training and education as this would have already been acquired and because of his previous SCADA experience and knowledge.

The present authors have evaluated this case based on the information from the IT Security Expert Advisory Group, (2005) and have derived a score using the capability model (as shown by Table 4 & 5).

Table 4. Terrorist Motive to Orchestrate Cyber-terrorism-Validated

Terrorist Motive Required for a Cyber-terrorist Attack in Australia	**Indicator**
Political/Motivation- For an individual terrorist or group to orchestrate a cyber-terrorist attack against Australia they initially would need to have acquired a very high level (e.g. equivalent score of 5) of anti-Australian sentiment with political motivation to spread their ideology or to generate change by creating fear through an attack using or targeting ICT.	No

Table 5. Cyber-terrorism SCADA Capability Mode -Validated

Terrorist Cyber-Capability Level Indicators Required for a Cyber-terrorist Attack in Australia	**Score Range**
Terrorist leaders and members with advanced ICT skill set- This level capability indicator requires terrorist leaders to have advanced knowledge of ICT including: TCP/IP, advanced cryptography, Botnets, Biometrics, and other associated security technologies.	4
Terrorists with advanced hacking tools and techniques- This capability level indicator would require education in ICTs and software training e.g. hacking tools and hardware to orchestrate an attack.	4
Access to new advanced ICTs- This capability level indicator involves terrorists or groups having access to new emerging technologies. E.g. biometrics, advanced encryption.	4
Advanced knowledge of SCADA systems- This capability level indicator involves terrorists having a high level of SCADA knowledge including; software engineering, middleware, application layer and backend.	5
Terrorist insiders within the organisation of selected target- this capability level indicator involves having a terrorist or member inside a critical infrastructure organisation such as power, gas, water etc, either within their IT department or operational control department.	5
Reconnaissance- this capability level indicator requires scanning and probing SCADA networks to find and detect SCADA vulnerabilities in order to prepare for attack.	1
Funding- this capability level indicator requires financial backing within the group to orchestrate attacks. This includes equipment, training, hiring, planning, organising, educating, etc.	2
Total Level of Cyber-Capability Indicators	Score =25/40

The score indicated from the Queensland case 2000 demonstrates how the model can be used for existing or future related cases in relation to cyber-terrorism.

STAGE 3 AS/NZS 27002:2006 CYBER-TERRORISM SCADA CONTROLS SUBSET

The AS/NZS 27002: 2006 cyber-terrorism SCADA controls subset is the final stage in the cyber-terrorism SCADA risk framework and has also adopted an existing risk standard approach for a SCADA environment. This subset provides the necessary controls which are required to reduce the vulnerability of an attack against an organisation's SCADA system. This subset (which is beyond the scope of this paper) presents the stages and the controls that are required to protect organisations from cyber-terrorism and gives organisations a baseline (low-level) methodology for reducing SCADA security threats.

The AS/NZS 27002:2006 cyber-terrorism SCADA controls subset has been based on the AS/NZS 27002:2006 risk standard and has been customised and modified to suit a generic SCADA environment (Standards Australia, 2006). The objectives and controls are to be implemented to meet the requirements identified in the first stage of the cyber-terrorism SCADA risk assessment subset. These controls will help reduce those risks which are identified in the cyber-terrorism risk assessment subset and provide a high level methodology to mitigate the threat of cyber-terrorism against SCADA systems within Australia.

The cyber-terrorism SCADA controls subset contains 11 security control clauses which are listed below. These clauses provide a generic methodology to reduce the risks which are identified in Stage 1 of the cyber-terrorism SCADA risk framework. Figure 1 describes the 11 clauses within this standard *(See Beggs and Warren 2008 for further details of stage 3)*:

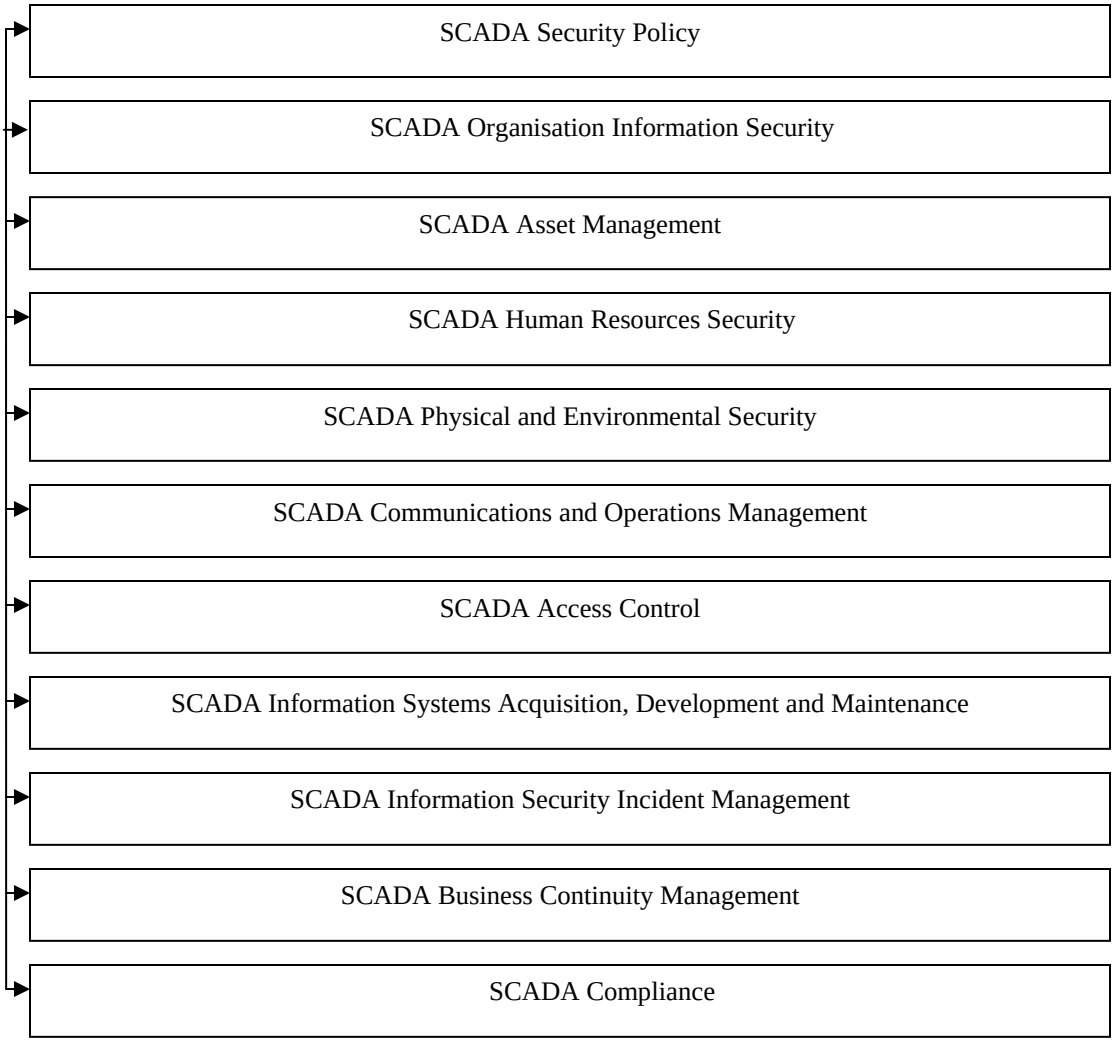

Figure 1 SCADA Controls to Reduce the Threat of Cyber-terrorism (Based upon Standards Australia, 2006)

INDUSTRY ADOPTION AND ACCEPTANCE FOCUS GROUP VALIDATION AND EXAMINATION

The framework presented above has been validated by a SCADA industry focus group. The results and findings from the focus group are discussed below providing further data in order to validate the frameworks' importance and significance within an industry based context (*See Beggs and Warren 2008 for additional focus group validation and results).*

Industry Focus Group Aim and Purpose

The focus group involved 5 participants from a SCADA "Tier 1 Top 5" engineering consulting company who contributed to the focus group in order to provide feedback and data on how widely the framework could be used within in industry and how the consulting company could use the framework to assist their clients who are owners and operators of SCADA systems within critical infrastructures.

Participant "A" was a certified security risk practitioner who had several years experience within the security industry. This participant had worked on various security projects within the critical infrastructure arena and has specialised certifications, accreditation and qualifications of risk standards. Participant "A" had extensive experience in conducting risk assessments and security audits as well as implementing and developing security policy. Participant "B" was a SCADA control systems engineer who had previous experience working with SCADA systems including SCADA system design, SCADA architecture and SCADA implementation across many different industry sectors. This participant was a senior SCADA expert in the field who had been involved in various SCADA projects in recent years within Australia and overseas. Participant "C" was another senior SCADA engineer who had worked previously for various SCADA vendors developing SCADA software and hardware. This participant had advanced knowledge of SCADA equipment and applications and had been designing and implementing SCADA systems for several years. Participant "D" was another senior SCADA control systems engineer who had worked on numerous SCADA projects within multiple critical infrastructure sectors. This participant had over 20 years experience with industrial control systems including SCADA and Programmable Logic Controllers (PLC's) and Distributed Control Systems (DCS) systems. Participant "E" was a junior control systems engineer who has experience in designing SCADA HMI screens and SCADA applications for industrial controls systems. This participant had a very high level knowledge of engineering coding and programming skills for customised SCADA applications for many different SCADA sectors.

Focus Group Study Theme

The focus group involved an experienced facilitator who assisted in moderating the discussion between all participants. The focus group presented a cyber-terrorism SCADA attack scenario which established the significance as well as the usability of the framework and its overall contribution to the research area. The focus group's aim was to collect data based around these discussion questions:

- Does the framework follow a process that organisations could easily adapt to measure and protect against the threat of cyber-terrorism to SCADA?
- How widely would SCADA asset owners, SCADA engineers or industry practitioners use the framework presented?
- If you are a SCADA asset owner or SCADA engineer and you needed to evaluate the likelihood of cyber-terrorism occurring against your SCADA system. How widely would you use the Cyber-terrorism SCADA Capability Assessment Model (Stage 2) of framework to measure this likelihood?
- Would there be any industry implications when using or adopting the framework?

Industry Focus Groups Findings and Results

The discussion and findings is based on how widely industry would adopt the cyber-terrorism SCADA risk framework. Participant "B" suggested that the "framework follows a process that addresses vulnerability". This participant believed that the proposed framework provides a "formal approach at identifying risks against SCADA." Participant "B" argued "that there is a need for a framework for SCADA engineers and consultants when identifying SCADA risks" such as cyber-terrorism. Such comments suggest that the framework has a valid purpose and can be of value to the SCADA community. Participant "B" argued that in the "past SCADA consultants have not followed a comprehensive approach in assessing these types of threats." Participant "B" claimed that with "previous risk assessments workshops" the participant had been involved in that "no formal approach was being used for SCADA." This participant gave an example regarding "regular password changes when employees leave the utility who are SCADA users." The participants claimed that "these types of processes were not readily adopted at plant sites that he had been involved in." Participant "B" suggested that the framework "provides a process that would encourage SCADA consultants to be more security aware and would enable them to perform a comprehensive and detailed risk assessment on SCADA systems." Participant "B" suggested "that industry and consultants require a framework to assess SCADA security risks." Also, the participant suggested that they had "not seen a framework that specifically addressed SCADA security risks." The comments from participant "B" once again reinforce the frameworks' originality, significance and overall contribution to knowledge and the SCADA community.

Participant "B" also argued that an "issue faced in using this framework may be the creditability of assessing outside organisations' ability to measure the cyber-capability of terrorist groups." However the participant agreed that if TISN or a trusted government security agency could be used to assess the cyber-capability of terrorist groups that "this would contribute to the overall creditability." The present authors explained that this was included as a

suggested procedure and guideline in the model and that creditability could be overcome by a trusted source such as TISN or ASIO. This once again reiterates the significance of having a cyber-terrorism steering group in order to assess and estimate scores within the cyber-terrorism SCADA capability assessment model.

Likewise, Participant "C" claimed that there may "be implications when implementing the framework on rather large installations when selecting hardware and equipment that may not be installed until three years." This participant suggested that capability of the "hardware may not be able to be updated in order to meet the growing threat level." The present authors suggest that technology will constantly being changing and that updating and reviewing of the entire model at least every 6 months or accordingly to each organisation's needs and requirement levels would assist in overcoming such problems. This suggests that the framework is adaptable to ongoing change and refinement and also demonstrates the model's flexibility with each individual organisation, providing even further validation and acceptance.

Also, Participant "D" suggested that there would be a "great deal of confidence in adopting the framework as there is no framework that exists" that addresses cyber-terrorism and SCADA risks. This participant believed that "educating users about the framework would be beneficial in the adoption process." The present authors agree with the participant's comments and suggest that the framework could be adopted relatively easily by educating SCADA engineers on the cyber-terrorism and SCADA risk process. Participant "D's" comments once again demonstrate that the framework is useful and significant for SCADA engineers and SCADA asset owners. This overall adds value to the framework's purpose, but more importantly to the overall research contribution.

Furthermore, Participant "A" argued that the framework provides an "original process" and "that there is no framework that deals with this type of threat." The participant claimed that the "framework demonstrated a "suggested process to mitigate risk." Participant "A" argued that once a "framework is launched then obviously through experience it builds." This participant suggested that the framework was "brilliant" and that adopting the framework "looks at a process that could be put into place." Participant "A" said that a "framework in place such as this had not been done before." Participant "A" argued that it's "on the tips, tongues, minds and heart of the corporate world and government security agencies all over the world." This participant believed that there was "a lot of merit" in the framework and its contribution. Also, the participant argued that it "provided a starting point that could be vertically integrated" into organisations. Likewise, "keeping it simple" was another suggested comment by Participant "A" who claimed that "government agencies are trying to get their head around the cyber-terrorism threat." The present authors strongly agree with such comments made by Participant "A" and believe that the framework provides a systematic and fluid process that could be simply used and adopted by industry and government. Participant "A" said that the framework gives "SCADA engineers an understanding of what risk assessment processes there are for SCADA." This ultimately again adds strong value to the overall validity, purpose and adoption phase of the framework within industry. Participant "A" also claimed that the framework is very useful as it gives "suggestion and viewpoints" and if the framework "could be rated out of 100 I would give it 500 as there is definitely merit in it." The participant's comments, reinforces the framework's validity and significance within the SCADA community.

Similarly, Participant "E" suggested that on "previous projects regarding SCADA security risk assessments they had never used a formal approach or framework in identify threats against SCADA." After adopting and using the framework proposed this participant believed "that it was of great benefit as it identified gaps and security issues that were not previously recognised" in assessing SCADA threats such as cyber-terrorism. This participant firmly agreed that the "framework was of great value and benefit." This highlights that the framework has subsequently been adopted on various projects within the SCADA "Tier 1 Top 5" engineering consulting company. This once again demonstrates the framework's overall significance and purpose, and also reinforces the framework's validity and industry acceptance and adoption.

Likewise, Participant "C" reinforced the use and acceptance of the framework and said "that in terms of assets owners, they would use the framework in order to determine the risks they face from threats including cyber-terrorism." Participant "A" said that "SCADA asset owners would use the framework because the threat of cyber-terrorism is evolving." However the participant claimed that many SCADA asset owners are "not aware of the framework for cyber-terrorism because the concept is so new." Participant "A" suggested that most "SCADA asset owners don't even know what cyber-terrorism means" and that "they have not ventured into this area." However, the participant suggested that "some major utilities companies are aware of this issue and would use the framework."

The participant argued "that it's an education and culture process and that there are people screaming down the door for this type of thing." Participant "A" said that the framework would "need to be engaged with SCADA engineers and that education would be required."

The present authors would like to acknowledge that the framework is actively being presented throughout industry which is providing the opportunity to educate SCADA engineers and SCADA asset owners of the threat of cyber-terrorism against SCADA systems. It also is encouraging SCADA asset owners to adopt the framework in order to assess security threats such as cyber-terrorism. Participant "A" also suggested that there was definitely a need for such a framework within corporate Australia." The present authors agree with the comments suggested by Participant "A" indicate that the framework provides a major contribution to all SCADA engineers and consultants. He has also encouraged all members of the SCADA community to embrace and acknowledge the real dangers faced from cyber-terrorism and other associated security risks, when adopting the framework.

On the other hand, there were some industry implications that were discussed within the focus group. Participant "D" claimed that "small organisations may not adopt the framework because it may be too costly to implement." This participant suggested that "certain types of industries that use SCADA systems may not see any benefit." For example, the participant suggested that organisations that "make plastic bottles using SCADA systems may not see any value any adopting the framework." Participant "D" agreed that these types of organisations may not be a subjected to a terrorist attack such as cyber-terrorism." Participant "C" also supported this comment by suggesting "that in some industries down time on SCADA systems and PLC's is not as critical as in other sectors." The present authors agree with both participants and suggest that the framework would be more suitable and appropriate for large organisations controlling critical infrastructure such as power, gas and water, etc. The present authors also agree that cost would be an implication for smaller organisations as they may not have the funding to carry out the SCADA risk process and the cyber-terrorism capability assessment model by funding and organising the cyber-terrorism steering group. These issues and implications would only be applicable to certain types of organisations. As the majority of SCADA systems are controlled by very large critical infrastructure organisations and therefore the framework should be targeted towards these types of infrastructures.

This is supported by Participant "B" who suggested that the "framework would be used in major process industries such as power, water oil and gas where any type of shut down is hugely costly." This participant also suggested "that the framework would be useful at the board level as they would be interested in risks that would shut down processes within the plant." The participant claimed that the framework "would support this as high risks could be identified" such as cyber-terrorism. Also, Participant "B" suggested the use of the "cyber-terrorism steering group" would be adopted if the organisations had the budget. This participant provided an example that "if cyber-terrorism was their number one risk", that "his organisation would definitely go ahead with acquiring the resources through TISN, and ASIO in order to make an assessment for the cyber-terrorism SCADA capability model." This once again demonstrates enormous value and significance for organisations to adopt the cyber-terrorism SCADA risk framework.

The main implications identified from participants within the focus group in regards to industry adoption included:

- Cost of implementing the framework;
- Education and cultural issues need to be considered when implementing the framework;
- Small organisations may not adopt the framework as it may not be suitable to their industry;
- The framework needs to be industry specific and targeted to larger organisations.

These implications would only be applicable to certain organisations and would not affect the overall purpose of the frameworks functionality usability and adoption within an industry based context.

Lastly, the industry focus group provided positive feedback on how widely the framework would be adopted by industry SCADA professionals. The results and findings have demonstrated how organisations and SCADA practitioners would use the framework and also how important a framework such as the one presented is needed within industry.

In summary, the main findings and results regarding the industry adoption phase of the model within industry has been identified by the focus group in order to provide final validation of the cyber-terrorism SCADA risk framework. Below is a summary of the results and findings:

- There is no framework readily available that address cyber-terrorism and SCADA;
- There is a great need within industry for a framework that deals with SCADA security threats such as cyber-terrorism;
- The framework would be most suitable for large process control organisations that depend on criticality for their operations;
- The framework maybe costly to implement for smaller organisations;
- The framework has merit and is of great value and significance within the SCADA industry;
- The framework would be widely accepted and used by many organisations that use SCADA systems.

CONCLUSION

This paper has presented a framework to measure and protect SCADA systems from the threat of cyber-terrorism within Australia which various experts from various industrial sectors have tested and validated as an effective means to identify Australian SCADA systems' vulnerabilities, terrorist' capabilities and the means to control factors to reduce terrorists' possibilities for conducting successful attacks against these infrastructure assets.

The industry focus group findings demonstrated how widely the framework would be used within industry and has suggested how significant and important the framework is needed within industry. The overall acceptance by industry once again provides the present authors and the research community with a framework that is highly regarded and valuable to all SCADA practitioners. These results and outcomes have assisted in addressing how to measure and protect SCADA systems from cyber-terrorist threats. The research developed is of great significance and value to the SCADA security community and to organisations that are controlling SCADA systems within Australia. The research has provided organisations with a methodology to measure and to protect against the threat of cyber-terrorism, but more importantly, has demonstrated the need for new counter-terrorism security models to assist with assessing new cyber security threats such as cyber-terrorism.

REFERENCES

Beggs, C. (2005) Cyber-terrorism A Threat to Australia? *Managing Modern Organisation with Information Technology- Information Resources Management Association (IRMA)* 2005 San Diego, USA, pp 472-475.

Beggs, C. & Warren, M. (2008) Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Australia, *The Journal of Information Warfare*, 7 (1), 24-35.

Denning, D. (2000a) Cyber-terrorism Testimony before the Special Panel on Terrorism Committee on Armed Services US House of Representatives, Georgetown University. Retrieved September 29, 2009 from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Internet Security Systems (2005) Assessment and Remediation of Vulnerabilities in the SCADA and Process Control Systems of Utilities. Retrieved October 27, 2009, from http://documents.iss.net/whitepapers/SCADA.pdf.

IT Security Expert Advisory Group (2005) Supervisory Control and Data Acquisition-SCADA Security Advice for CEOs," Trusted Information Sharing Network. Retrieved November 7, 2009, from http://www.tisn.gov.au

Krutz, R. (2006) *Securing SCADA systems*, Wiley Technology, Indianapolis.

Lemos, R.(2002) E-terrorism: Safety: Assessing the Infrastructure Risk, CNET Network, Retrieved May 20, 2009, from http://news.com.com/2009-1001-954780.html

New York Times (2007) A Cyber-blockade in Estonia, The New York Times. Retrieved July 23, 2009, from http://www.nytimes.com/2007/06/02/opinion/02sat3.html

Slay, J. & Koronios, A. (2006) *Information Technology Security & Risk Management*, John Wiley & Sons, Milton, Qld.

Standards Australia (2004) AS/NZS 4360:2004 Risk Management. Retrieved April 12, 2009, from http://www.standards.com.au

Standards Australia (2006) AS/NZS 17799.2006 Information Technology- Security Techniques-Code of Practice for Information Security Management. Retrieved April 12, 2009, from http://www.standards.com.au

Telegraph (2008) School Boy Hacks into Tram System, Telegraph. Retrieved October 2, 2009, from http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-city's-tram-system.html

Trusted Information Sharing Network (TISN) (2008) What is SCADA. Retrieved October 2, 2009, from http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/e-Security#_What_is_SCADA?

APPENDIX

Gazprom Case 1999

In 1999, hackers broke into Gazprom a gas company in Russia. The attack was collaborated with a Gazprom insider. The hackers were said to have used a Trojan horse to gain control of the central switchboard which controls gas flows in pipelines, although Gazprom, the world's largest natural gas producer and the largest gas supplier to Western Europe, refuted the report (Denning 2000).

Queensland Case 2000

In 2000, in Queensland Australia, a 49 year old man, Vitek Boden hacked into an industrial control system using the Internet, a wireless radio and stolen control software and consequently managed to release millions of litres of sewage into the river and coastal waters of Maroochydore in Queensland, Australia (Lemos, 2002). After resigning from his position at Hunter Watertech and later being refused a new position with Maroochy Water Services, he began a sabotage campaign against the sewerage management system and made 46 intrusions. Each time he gained access to the system, the laptop assumed the functions of a pumping station and was able to access the nodes governing the control of the sewerage system operations. As a result, marine life died, the creek water turned black and the stench was unbearable for residents. The unauthorised intrusions costs $13,000 in clean up and $176,000 in extra monitoring and security of the system, also, the incident resulted in an extensive and costly in-house investigation and media activity and a loss of Maroochy Water Services' reputation over a five month period (IT Security Expert Advisory Group, 2005).

SQL Slammer Case 2003

In January 2003, an Internet based worm called SQL Slammer was released. Slammer generated considerable network traffic denying service to all other network users. Slammer exploited the vulnerability in a Microsoft database product. The SCADA system that utilised this product was potentially vulnerable to the worm. At the Davis Besse nuclear power plant in Ohio, worm activity on the Process Control Network blocked SCADA traffic causing the operators to lose some degree of control of the system. As a consequence, the plant's Safety Parameter Display System and Plant Process Computer was disabled for four hours, fifty minutes and six hours and nine minutes respectively (IT Security Expert Advisory Group, 2005).

Estonia 2007

In April 2007 the Russians attacked Estonia computer infrastructure forcing many websites to shut down which inflicted huge losses to Estonia's economy. According to the New York Times the assault of Estonia's virtual society began after Estonian authorities moved a statue of a Soviet soldier from a central park in Tallinn to a military graveyard further from the centre city. For many Estonians, the statue was another reminder of Soviet invaders who took their homes at Stalin's orders. Russians and Estonians of Russian descent immediately took the streets protesting. Removing the statue was a sign of disrespect for Soviets who battled the Nazis in World War II. Shortly after the protest, waves of unwanted data quickly clogged the Web sites of the government, business, banks and several newspapers, shutting down one branch of their computer network after another. The attacks lasted for over a month and caused major disruption and loss to Estonia's economy (New York Times, 2007). These attacks

demonstrate the impact of information warfare between two nation states. Although these attacks were politically motivated, the attacks did involve one state attacking another in a warfare scenario as well as causing minimal fear or harm to anyone and therefore cannot be classified or labelled as cyber-terrorism.

Polish Trams 2008

In 2008 a teenage boy hacked into a Polish tram system and used it like "a giant train set, causing chaos and derailing four vehicles. The 14-year-old, described by his teachers as a model pupil and an electronics "genius," adapted a television remote control so it could change track points in the city of Lodz. Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents (Telegraph, 2008). Such cases demonstrate the capability for individuals to carry out such attacks although this case did not demonstrate signs of political motivation, it does sever to highlight the possibility of cyber-terrorism occurring.

COPYRIGHT

Christopher Beggs and Matthew Warren ©2009. The author/s assign Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors