Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening

Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening[1]

Carol Taylor, Axel Krings and Jim Alves-Foss
Computer Science Department
University of Idaho, Moscow, Idaho 83844
{ctaylor, krings, jimaf}@cs.uidaho.edu

Abstract

In this paper we present a new cyber security assessment approach, which merges Survivability System Analysis (SSA) with Probability Risk Assessment (PRA). The method adds quantitative information to the process oriented SSA method, which assists with decision making among security options. Our technique is currently being developed for power industry cyber security assessment and hardening. A substation example is presented, with hypothetical risks and costs from several attack scenarios. Our technique features self-assessment, risk estimates based on actual data and quantifiable inputs for decision analysis. This assessment method is particularly well suited to hardening critical infrastructure systems against cyber attack and terrorism.

Keywords: *Computer Security, Risk Assessment, Cyber Terrorism, Infrastructure Protection*

1. Introduction

The lack of computer security is a widespread problem that crosses all geographic, political and societal boundaries. Malicious computer activity flourishes in spite of enormous amounts of time and resources applied to the problem. The popular FBI/CSI crime survey shows an unabated increase in incidents originating from the Internet with total losses at over 450 million [22]. While these statistics show an alarming trend in the number of external incidents and financial losses due to cyber crime, they say little about our susceptibility to cyber terrorism, an issue of increasing concern. Pollitt [21] claims that cyber terrorism combines two commonly held fears: that of random, violent victimization and a distrust of computer technology. According to Denning [7], cyber terrorism differs from most other types of computer attacks in that it is motivated by political, religious or ideological reasons and its intended purpose is to influence or coerce governments towards specific actions. Others have commented on the equalizing effect of cyber terrorist attacks whereby groups with limited resources can reap disproportionate gains against more powerful adversaries [28]. The typical terrorist strategy of attacking a few individuals and relying on public fear to pressure the government into action [8] is well suited to attacks against the cyber world. It would take relatively few resources to attack a specific target, e.g. a large network or infrastructure system, and cause widespread fear from a major or prolonged service disruption [8].

In assessing the US's vulnerability to cyber terrorism we need to ask two questions:

> Are there infrastructure targets vulnerable to terrorist attacks?
> Are there groups with both skills and motivation to perform acts of cyber terrorism? [7]

Several authors believe overwhelmingly that our infrastructure systems are vulnerable to cyber terrorist attack [7,23,28]. Answering the second question is more difficult. At present time, there has not been a catastrophic cyber terrorist incident since terrorists have opted for physical means of achieving their goals such as exploding car bombs and hijacking planes [7]. Yet, many feel it is only a matter of time before terrorists cause a major infrastructure failure leading to potential death and economic disruption. The belief is that future terrorists will grow up in a computer-based world with easy access to sophisticated attack tools capable of inflicting damage at relatively little risk to themselves [7,23].

Examining the threat of cyber terrorism to the electric power industry raises several issues. Both physical and cyber security threats have concerned the power industry for a number of years. The electric power infrastructure is one of the eight critical infrastructure identified by President Clinton's Commission on Critical Infrastructure Protection [20]. Electrical energy along with communications were identified as the most critical components of the infrastructure to the maintenance of American commerce and society [20].

Recent changes in the electric power industry have decreased the reliability of the North American power

[1] Portions of this work were funded by grant #60NANB1D0116 from the National Institute of Standards and Technology, U.S. Dept. of Commerce.

grid and increased its vulnerability to disruption from cyber attack. The major overriding change is the on-going restructuring as a result of de-regulation begun in the early 90's. This has resulted in industry consolidations and downsizing leading to instability in the workforce and the creation of a potential pool of disgruntled employees [20]. Security directors estimated that 75% to 80% of the security incidents are caused by persons within the organization [10]. Re-organization has also led to the introduction of new information systems for electronic data exchange. This requirement has resulted in greater connectivity between previously separate entities spreading the vulnerabilities that come with sharing potentially sensitive data over a network. The growing use of automated electronic devices in substation operation increases the risk from both insider and outsider intruders. Supervisory Control and Data Acquisition (SCADA) are widely used to control critical power generation and transmission equipment [19]. SCADA systems offer an attractive target for their disruptive power since intruders could modify the data used for operation or control of power equipment. The vulnerability of SCADA systems increases when connected to corporate networks with external access. Other electronic devices increasingly being used in substation control include Integrated Electronic Devices (IED's), Programmable Logic Controllers (PLC) and substation controllers. Additional factors that contribute to the growing intruder threat include the wide availability of hacker tools, the lack of security awareness and the increase in terrorist incidents targeting Americans [18,19].

In this paper we present an approach for the assurance assessment of power substations that will assist substation hardening against cyber attacks including terrorist attacks. Our approach, Risk Analysis and Probabilistic Survivability Assessment (RAPSA), combines Survivability System Analysis (SSA) from computer survivability with Probabilistic Risk Assessment (PRA) from dependability [27]. The goal is to incorporate the best characteristics of both methods into a single process developed for power industry substation assessment. While the current target is the power industry, this method is being developed as a general process that could be applied to other industries. The RAPSA process exhibits several notable characteristics, that distinguishes it from other security assessment methods:

- Strong self-assessment tool to minimize reliance on security experts
- Risk estimates based on actual data
- Quantifiable outputs for cost/benefit cyber security analysis

This preliminary work overviews the RAPSA process and discusses its applicability to the general problem of hardening heterogeneous networks against cyber intrusions. An example is presented of applying RAPSA to a power substation. Future work will discuss the formal representation of a model for the merged survivability/risk process.

The paper covers survivability assessment for electric power substation hardening. Section 2 describes how survivability and PRA are merged into the RAPSA process. Section 3 applies the process to the assessment of a power substation. Alternative approaches are discussed in Section 4 and our conclusion are outlined in Section 5.

2. Survivability + PRA = RAPSA

As presented in the previous section, threats from cyber attacks to infrastructure computer systems are an increasing concern as the complexity of these systems grows and our reliance on them becomes critical for national health and safety [20]. The sheer size and geographic distribution of these systems prohibits hardening all system components against cyber attack. A survivability analysis will enable the partitioning of a system into components critical to the mission objectives and those components of lesser importance. Risk analysis will allow the quantification of cyber threats and, based on mitigation strategies identified in the survivability analysis, outline mitigation strategies dealing with those threats. This section discusses the merging of attributes from both Survivability System Analyses and Probability Risk Assessment. First, we separately review SSA and PRA and then describe our technique for merging these two processes.

2.1 Survivability System Analysis (SSA)

Survivability evolved out of the need to protect systems connected to unbounded[2] networks. The lack of centralized control and the distributed nature of these networks makes the task of hardening systems connected to these networks nearly impossible [10]. Computer system survivability emphasizes continued operation, though in a degraded mode, in spite of successful compromise or natural failure. Survivability is typically defined as the capability of a system to complete its mission in a given time frame even if portions of the system are compromised due to accident or attack [10]. Survivable systems must therefore be able to preserve essential services under attack or failure, recover full services within a reasonable time, and ensure survivability

[2] Unbounded networks are large, distributed networks with ill-defined boundaries and non-centralized control.

given the unbounded network environment typical of today's computers [10]. In this work, we ignore natural[3] failure events and concentrate on deliberate cyber attacks since our concern is mitigating the effects of cyber terrorism. The mission is often subject to interpretation and covers a number of high level requirements. Similarly, the concept of time is totally dependent on the target system and will vary with each system.

A key survivability concept is the identification of essential services along with essential properties in support of those services. Among the essential properties of interest are integrity, confidentiality, availability, reliability or performance requirements. Essential services are those services that are deemed critical to the organization's mission. These services must be preserved over less critical services, which may be temporarily suspended during or after an attack [10]. Survivable systems must exhibit four key properties in their capability to withstand attacks:

Resistance – attack repel capabilities
Recognition – attack detection or damage evaluation
Recovery – full service restoration
Adapt/Evolve – improve survivability based on attack knowledge

The SSA method defines a process that seeks to thoroughly define survivability properties of systems, threats to survivability and modifications to enhance survivability. SSA is a four step process that implements survivability assessment of a given system [10]. Step one seeks to understand mission objectives, system requirements and risks. Step 2 identifies essential services that must be maintained during attack. During step 3 the threat is assessed based on intrusion scenarios. Step 4 identifies the vulnerabilities to essential components and analyzes them for properties of resistance, recognition and recovery. The results of the so-called "3 R" analysis, i.e. steps 1 through 3, is summarized in a survivability map [10]. This provides management with a guide for survivability, evaluation, and improvement.

The primary advantage of survivability analysis as applied to large distributed networks (such as those typical of infrastructure systems) is the focus on the preservation of essential services as opposed to all services. This allows an organization to allocate their security resources where they are needed and devise strategies to continue operation under adverse conditions. One problem with survivability as an analysis technique is its lack of quantification. Without quantification, it is difficult to measure system survivability and determine the success of the system in meeting its survivability objectives. The lack of survivability measures was discussed at a recent survivability workshop [29] and was acknowledged as an area in need of further research.

2.2 Probability Risk Assessment (PRA)

PRA is a technique that seeks to define and quantify the probability that an adverse event will occur [14]. Quantitative risk assessment utilizes probabilities to determine the likelihood of events. Probabilities are frequently calculated from statistical sampling, historical records or experimentation. In cases where these "objective" sources are sparse, "subjective" sources are often used in the form of expert opinion [14]. For assessing the threat from cyber attacks, risk becomes the likelihood that a given actor will exercise a particular system vulnerability [5]. Ultimately, the goal of a PRA for cyber security is to identify the potential threats and system vulnerabilities, quantify the likelihood of those threats and produce mitigation strategies based on both the risk and associated costs. In general, a PRA is conducted in three stages [14]: Risk identification, risk quantification and risk evaluation and acceptance (Table 1).

Table 1. Three stages of Probability Risk Assessment

Stage	Question	Actions
1 Risk Identification	What can go wrong?	Identify risk source
2 Risk Quantification	What is the likelihood it would go wrong? What are the consequences?	Assess probabilities subjective, or objective Model causal relationships and their impacts
3 Risk Evaluation and Acceptance	What can be done? What are the options and trade-offs?	Create policy options Trade-off analysis of risk and cost/benefits of mitigation

[3] Failure from natural causes such as weather will likely be isolated events of limited scope. Because of the resiliency of the power grid to these types of failures the power loss will likely be contained.

PRA has long been used in safety related fields such as nuclear energy, rail and air transportation where the consequences, of accidents can be catestrophic [16]. The use of PRA to evaluate the risk of cyber attacks is not well established for reasons that will be discussed later in this section. A number of methods have been used in identifying risks to an organization. Most techniques focus on enumeration of initiating events through familiarization with the system and its potential vulnerabilities. For safety related systems, FEMA, HAZOPS, and PHA have been used to identify events [16].

Two common techniques for modeling risks and causal relationships are event and fault trees. Event trees use a forward search technique to identify various outcomes of an initiating adverse event. States in the forward search are depicted as branches showing the success *($1-P_i$)* or failure *(P_i)* of a protection mechanism. A path's probability is found by multiplying together the branches of the path [16]. Event-trees help understand how an adverse event is affected by mitigating mechanisms and permits the construction of probabilities for each path. Fault trees use a backward search that begins with an undesirable event and uses Boolean logic to describe the combinations of basic events that could cause the top-level event. Fault tree analysis examines the causes of failures, not the failures themselves and relies on other methods for failure identification [14,16].

A final step in a PRA is to utilize the risk probabilities for the adverse events and perform a trade-off analysis according to the risks and costs of mitigating those risks. In real systems there are often competing objectives and genuine constraints on the measures available for risk mitigation. Several techniques have been proposed for optimizing decisions under competing objectives such as Multiobjective Tradeoff Analysis (MOTA) and Partitioned Multiobjective Risk Method (PMRM) for analysis of the risk of extreme events. For simpler risk decisions, simple decision tree analysis can also prove useful [14]

The benefits from performing a PRA for the assessment of cyber attacks include numeric estimates for the allocation of security resources and an enhanced understanding of the security vulnerabilities and threats. Yet, despite the potential benefits, risk analysis for computer security has more detractors than supporters and is typically not done. A significant problem appears to be a lack of cyber security data, which presents a major roadblock to risk quantification [3]. The lack of a historical database of cyber security incidents creates problems for insurers and other industries that are trying to assess computer security risk [13]. Reasons for industry resistance to the disclosure of security incidents include fear of liability, loss of reputation and competition issues [3,12]. The reluctance to share cyber security data is a problem that transcends risk assessment and is a significant security barrier to securing the power infrastructure [12,20]. Other problems with cyber security assessment of risk includes the difficulty of analyzing the risks and mitigation strategies for large complex networks [5] and the inaccuracies associated with the expected loss from security events [1,5].

2.3 RAPSA Process Description

The previous two sections detailed the techniques of SSA and PRA, which have both been used to assess computer security. Individually, both SSA and PRA have strengths and weaknesses in evaluating a system's vulnerability to cyber attacks and suggesting corrective actions. While the individual methods are useful, we feel that a merged process would combine the strengths of both SSA and PRA and result in a better assessment process leading to more robust defenses against cyber attack. We envision a four stage RAPSA analysis process as follows:

Stage 1 – System Self-assessment

An analysis team performs a self-assessment to understand system mission objectives.

Partition the system into services that are essential to the mission and those services that are non-essential.

Stage 2 – Threat Identification

Threats from cyber attacks are enumerated for the essential services identified in the previous step.

Intrusion scenarios/ attack stages are outlined for the essential services.

Vulnerabilities associated with each intrusion scenario are documented.

Stage 3 – Risk Quantification

Quantify the risks for each intrusion scenario.

Event/fault trees will be used where needed to assist with understanding how attacks can be neutralized.

Mitigation mechanisms will be proposed.

State 4 – Risk Mitigation Trade-off

Several types of tradeoff analyses are possible such as Partitioned Multi- Objective Risk Method (PMRM) or simple Decision Tree Analysis.

Produce survivability map including risks and costs for mitigation strategies.

3. RAPSA Assessment for the Power Industry

In looking at the threats of cyber attacks to the power infrastructure, multiple layers of abstraction are possible. The power infrastructure is comprised of interconnected networks for the generation, transmission and distribution of power. While other approaches have proposed a top down solution to hardening the power infrastructure by simulation [4] or models of network control systems [26], our strategy is to understand the threats from the bottom up. Since the substation was identified as one of the most vulnerable components in the power grid [18], we selected the substation as an example for studying cyber threats and understanding how a substation could be hardened for survival against intrusions. Detailed knowledge of the vulnerabilities at the lowest layer of abstraction will assist us in understanding how cyber terrorists could penetrate the system and ultimately cause widespread damage.

Table 2. Regular power substation distribution tasks

Regular Power Distribution Tasks	**Essential Service**	**Non-essential Service**
- Control operator monitors SCADA control system – no adjustment needed	X	
- Control operator makes adjustments to SCADA[4] in response to RTU information	X	
- Control operator makes adjustments to SCADA from a remote access point	X	
- Control operator updates corporate computer with distribution data		X

In the following subsections an example of a simple RAPSA analysis of a substation is presented. It should be noted that the scenario is purely hypothetical. The selection of essential services may be arguable. Furthermore, the numerical values and costs used have no technical validity and are for demonstration purposes only.

3.1 Power Substation Assessment

Applying the RAPSA approach to a hypothetical power distribution substation will illustrate the method. In a distribution substation power is "stepped down" from the high voltages used for transmission to the lower voltages needed for customer distribution. Table 2 lists the regular usage tasks for the delivery of power to customers. In Stage one, the mission objectives are stated and essential services are identified. For a distribution substation, the mission is fairly straightforward – deliver power to customers. Three out of the four identified regular usage scenarios were selected as essential to the mission (Table 2). A non-essential service, which could be postponed, is the communication status information to corporate computers.

Stage two involves outlining the attack threat to the distribution tasks presented in Stage one. Table 3 presents attack scenarios against the distribution services of the power substation. While it is vulnerable to many cyber threats as outlined in Oman et al [19], two attack scenarios were selected as being representative of the types of cyber threats to distribution substations. One attack scenario involves an external intruder disrupting distribution and the other demonstrates how an insider could innocently provide access to an outside entity, which would similarly lead to a disruption of distribution. Since both scenarios lead to access of the internal substation systems that connect the electronic devices, all of these devices are at risk and considered vulnerable.

Table 3. Attack scenarios and system components affected

Attack Scenario	Affected Components
Scenario #1 – A hacker discovers the phone number of a modem connected to the substation computer. Login information is acquired through social engineering or other means, password attack. Intruder gains access to the system	- Electronic devices, IED's, Controllers or SCADA system - Data altered or destroyed, devices reset, communication blocked or re-routed
Scenario #2 – Employee is tricked into installing a game that contains a Trojan horse program. A back-door into the system is created, the program author is notified and gains access to the system	-Electronic devices, IED's, Controllers or SCADA system - Data altered or destroyed, devices reset, communication blocked or re-routed

Stage three involves quantifying the risk for each intrusion and suggesting mitigation mechanisms. In the absence of historical data or statistical sampling, expert opinion is solicited for producing damage risk estimates. One approach is to construct a distribution by the fractile method (See [14] for details). The fractile method partitions the [0,1] probability axis into sections, the fractiles, which are then associated with outcomes. Experts provide assessments for each fractile outcome. The probability density function (pdf) and cumulative density function (cdf) are constructed from subjective probability

[4] SCADA includes all IED and other programmable devices.

estimates. The expected or mean value of the damages from an intrusion is found by the following equation:

$$E[X] = \sum_{i=1}^{n} p_i x_i$$

where n is the number of fractiles, x_i's are the consequences and p_i's are the probabilities of an event.

Ideally, more than one expert will provide input, for each attack scenario. We show hypothetical estimates for attack Scenario 1, the external intruder, from one expert:

Scenario 1- External Intruder Gains Access to the SCADA System

Fractile	% Power Disruption	Explanation
.0	0	Best, no loss
.25	10	Small loss, 10%
.50	25	Medium damage
.75	50	More damage, 50 %
1.00	75	Worst case, 75% loss

Once the estimates from the expert(s) are obtained, the expected value of the disruption of distribution power can now be computed. This value represents the risk of damage under the current system configuration. The expected risk can be computed as follows:

$$E[X] = .25\left[0 + \frac{(10-0)}{2}\right] + .25\left[10 + \frac{(25-10)}{2}\right] + .25\left[25 + \frac{(50-25)}{2}\right] + .25\left[50 + \frac{(75-50)}{2}\right]$$

$$= .25(122.5) = 30.6$$

After implementing mitigating alternatives, new risk estimates are typically made. The survivability map augmented with these estimates is shown in Table 4.

For each of the mitigation options, the expert(s) provide revised risk estimates based on the decrease in power disruption risk as a result of the mitigation actions. Costs of each option can now be compared along with the reduction in risk.

After the mitigation strategies are outlined, the last step is to perform a decision analysis. Because there are so few mitigation strategies in this example, a simple decision tree will be constructed. In practice, risk analysis of cyber attacks will generate a greater number of scenarios and mitigation options. Multiobjective Tradeoff Analysis will assist in the optimization of conflicting objectives for more complex situations. Table 5 lists the hypothetical costs or losses associated with three levels of risk under three system states, Current System, Mitigation #1, and Mitigation #2.

Table 4. Survivability map, risk and cost estimates for attack Scenario 1

Attack Scenario	Resist	Recover	Risk	Cost/Year1
Intruder gains access by remote modem into SCADA system	Current: - regular modem, weak password, no system logging	Current: - Figure out intruder damage, reset devices in substation, restore SCADA data from backups	30.6	0
	Mitigation #1 - Dialback modem, no password sharing, no single system password, system logging	Review audit logs for intrusion evidence Restore SCADA data from backups	18.6	6,000
	Mitigation #2 - Restrict dial-in user actions, restrict user ID to time of day, intrusion detection system	Examine intrusion audit logs for access Restore SCADA data from backups	13.4	20,000

Table 5. Cost of three states under three risk levels

System State	Costs	Risks
Current System	40,000	40
	75,000	50
	100,000	10
Mitigation #1	24,000	40
	36,000	50
	44,000	10
Mitigation #2	25,000	40
	30,000	50
	40,000	10

Figure 1 shows the costs laid out in a decision tree representing three cost options at three different disruption levels.

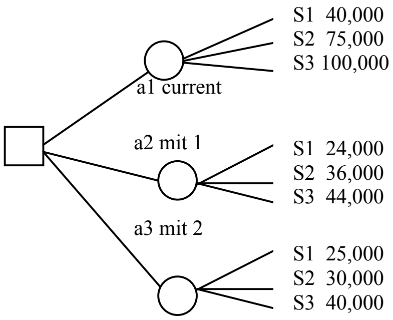

Figure 1. Decision tree

Computing the optimum damage mitigation option, we calculate the expected value of each of *n* alternative system states, a_i

$$E[a_i] = \sum_{j=1}^{n} p(s_i) u_{ij}$$

where $p(s_i)$ is the probability associated with scenario s_{i} and the cost of each pair $(a_{i\ ,}\ s_{\mathrm{j}}\ )$denoted by, u_{ij}

$$E[a_i] = \sum_{j=1}^{3} p(s_i) u_{ij} \ ,$$

i = 1 to number of alternatives

$$\begin{aligned} E[a_1] &= .4(40{,}000) + .5(75{,}000) + .1(100{,}000) \\ &= \$63{,}500 \end{aligned}$$

$$\begin{aligned} E[a_2] &= .4(24{,}000) + .5(36{,}000) + .1(44{,}000) \\ &= \$32{,}000 \end{aligned}$$

$$\begin{aligned} E[a_3\ ] &= .4(25{,}000) + .5(30{,}000) + .1(40{,}000) \\ &= \$29{,}000 \end{aligned}$$

The best alternative from the decision tree analysis based on minimal costs is $a_{3,}$, i.e. Mitigation #2.

3.2 Benefits of RAPSA

RAPSA offers several benefits in its combined approach of survivability and risk analysis. By incorporating numeric risk estimates for attack scenarios before and after mitigation strategies, comparison is possible between the different strategies. While estimates from experts may not accurately reflect actual risk, the major value from the risk estimates are to see the risks from different impact levels and compare costs from various hardening approaches. The result of following the SSA method is a survivability map with recommended mitigation strategies for system resistance, recognition and recovery. Yet for companies faced with a limited security budgets, the cost of different options, which is not included in a survivability map, is important. We believe that the numeric risk and cost estimates from conducting a PRA add significant value to the standard survivability map.

Another benefit of RAPSA is the emphasis on system self-assessment. The power industry's lack of security expertise and lack of cyber security awareness has been cited as an obstacle to securing these infrastructure systems [20]. We suspect other infrastructure industries have a similar lack of cyber security expertise. Consequently, it is extremely important to foster an awareness of security and build expertise within the individual companies that are vulnerable to cyber attack. SSA assumes there will be a team of security experts available to assist with the analysis. RAPSA assumes the opposite and tries to incorporate security assessment knowledge into the process so that minimal reliance on outside assistance is needed. The goal is to create teams capable of performing assessments on an on-going basis.

4. Related Work

Survivability system analysis was developed at CMU specifically for the assessment of unbounded networks [10]. It appears to have a great deal of merit for identifying infrastructure system vulnerabilities and proposing solutions under the system requirements of resistance, recognition and recovery.

Simulating large systems is another technique for discovering vulnerabilities and recovery mechanisms. Byon [4] showed how the power industry could be modeled using the EASEL simulation language. Sullivan et al [26] used a control architecture to model recovery for the US Payment system. Our approach differs substantially from these studies in that we believe a thorough understanding of the vulnerabilities and security challenges at the lowest level through real data is necessary before high level models can be built.

Other related work uses standalone risk assessment for cyber system security. In Freeman [11] a large heterogeneous network is analyzed in a top-down system wide approach. Drake et al [9] uses a risk assessment method and firewall application. Another study looks at the development of a software tool kit for automatic generation of fault and event trees [6]. All of the studies demonstrate that risk assessment is useful for the determination of threats. However, some of the cost estimates appear doubtful in [9] and it is unclear how the risk methodology used in [11] can be extended to other systems. Part of the problem with standalone computer security risk assessment is that it is difficult to relate the risks to the functionality of the system. Some system components may be assessed to be high risk but contribute little to the overall mission of the organization. Combining a survivability approach, which first isolates essential services, overcomes this problem.

5. Summary

The merging of two assessment techniques was presented. At this time, findings are preliminary since the RAPSA technique is under continuing development. Results from initial experiments using RAPSA showed that it added information in the form of risk and cost estimates that could assist with hardening a computer system against cyber attacks. Our substation example from the power industry illustrated its usefulness in identifying cyber attack threats and proposing mitigation activities. Ultimately, successful solutions to securing systems will incorporate technical and human-centric components. We, and others [3,24], feel that most computer security solutions over-emphasize technology while ignoring human contributions. We believe educating operators on cyber security vulnerabilities and intruder tactics is as important as installing the latest security product. In RAPSA, we incorporated a dual human/technical solution.

The results presented showed hypothetical risk estimates for an example problem. Future studies will produce risk figures from security experts as well as estimates from statistical sampling of the power industry and/or other historical data. Our interest in gathering risk information is not to estimate how vulnerable the infrastructure is to cyber terrorist attack, but how to proceed towards survivability maximizing benefits while minimizing cost.

6. References

[1] Anderson, R. *Security Engineering*: A Guide to Building Dependable Distributed System, Wiley Computer Publishing, 2001.

[2] Bier, V., Y. Y. Haimes, J. H. Lambert, N. C. Matalas, and R. Zimmerman, "A survey of approaches for assessing and managing the Risk of Extremes", *Risk Analysis*, Volume 19, No. 1, 1999, Pages 83-94, Society for Risk Analysis, http://www.kluweronline.com, 1999.

[3] Blakley, B., E. McDermott, D. Gear, "Information security is information risk management", NSPW, Cloudcroft, New Mexico, Sept. 2001.

[4] Byon, I. Survivability of the U.S. Electric Power Industry, Masters Thesis, CMU, 2000.

[5] Cohen, F. "Risk management or risk analysis", http://all.net/journal/netsec/9703.html, 1997.

[6] Craft, R., G. Wyss, R.. Vandewart, D. Funkhouser, "An open framework for risk management", *Proccedings of the National Information Security Conference*, 1997.

[7] Denning, D. "Is Cyber Terror Next?", Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.html, Sept. 2001.

[8] Devost, M.G., B.K. Houghton, N.A. Pollard, "Organizing for information warfare, the truth is out there", Terrorism Res. Center, http://www.terrorism.com, 1997.

[9] Drake, D. and K. L. Morse, "Applying the Eight-Stage Risk Assessment Methodology to Firewalls," in *Proceedings of the 13th Annual Computer Security Applications Conference (ACSAC'97),* Pages 44-52, IEEE, 1997.

[10] Ellison, R. J., R. C. Linger, T. Longstaff, and N. R. Mead, "Survivable Network Systems Analysis: A Case Study," *IEEE Software,* July/August 1999, 70-77.

[11] Freeman, J. W., T. C. Darr, and R. B. Neely, "Risk Assessment for Large Heterogeneous Systems," *in Proceedings of the 13th Annual Computer Security Applications Conference* (ACSAC'97), Pages 44-52, IEEE 1997.

[12] Gent, M. R. "Securing our Infrastructure: Public/Private Information Sharing", Testimony of Michehl Gent, President and CEO of NERC, 2002.

[13] Haimes, Y.Y., J. H. Lamberk, "When and How you can specify a probability distribution when you don't know much", *Risk Analysis*, Volume 19, Number 1, 1999, Society for Risk Analysis, http://www.kluweronline.com, 1999.

[14] Haimes, Y., *Risk Modeling, Assessment, and Management*, John Wiley and Sons, 1998.

[15] Hammitt, J. K. and Alexander I. Shlyakhter, “The Expected Value of Information and the Probability of Surprise,” *Risk Analysis*, Volume 19, Number 1, 1999, Pages 135-152, Society for Risk Analysis, 1999. URL: http://www.kluweronline.com.

[16] Leveson, N. G., *Safeware: System safety and computers,* Addison Wesley Publishing Co., 1995.

[17] NERC, “An approach to action for the electricity Sector, Ver. 1.0”, NERC, Wash. D.C., June 2001.

[18] NSTAC, “Electric power risk assessment”, 1997, http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html.

[19] Oman, P. E. O. Schweitzer, III, and J. Roberts, “Safeguarding IEDS, Substations and SCADA Systems Against Electronic Intrusions,” Technical Report, Schweitzer Engineering Laboratories, Inc., Pullman, Washington, U.S.A., 2001.

[20] PCCIP, “Critical foundations to protect. America’s infrastructures”, Report from the President’s Commission on Critical Infrastructure Protection, 1997.

[21] Pollitt, M.M., Cyber terrorism fact or fancy?”, FBI Laboratory, http://www.crime-research.org/eng/library/cyber1.htm, 1997.

[22] Power, R. “Computer security issues and trends”, CSI/FBI Computer Crime and Society Survey, CSI, 2002.

[23] Shimeall, T., P. Williams, C. Dunley, “Countering Cyber War”, *Nato Review*, Winter 2001/2002.

[24] Stidham, J. “Can hackers turn your lights off?”, Sans Institute, rr.sans.org/hackers/lights.php, Sept. 2001.

[25] Stoneburner, G., A. Goguen, A. Feringa, “Risk management guide for information systems”, SP 800-30, NIST, US Dept. of Commerc, 1999.

[26] Sullivan, K., J.K. Knight, S. Geist, “Information survivability control systems”, *Proceedings of the 21st International Conference on Software Engineering,* pp. 184--193, May 1999.

[27] Taylor, C. S., A. W. Krings, W. S. Harrison, N. Hanebutte, “Merging survivability system analysis and probability risk analysis for security assessment”, *Proceedings of the International Conference on Dependable Systems and Networks,* Wash. D.C., June 2002.

[28] Vatis, M., “Cyber attacks during the war on terrorism: A predictive analysis”, Inst. for Sec. Tech. Studies, Dartmouth College, Sept 22, 2001.

[29] Voes, J. “Ten challenges in information survivability”, in *Proceedings of ISW2001*, Vancouver, Canada, 2002.