CYBERCRIMES AGAINST THE ELECTRICITY INFRASTRUCTURE: EXPLORING HACKER AND INDUSTRY PERCEPTIONS

by

AUNSHUL REGE

A Dissertation submitted to the

Graduate School-Newark

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Criminal Justice

Written under the direction of

Dr. Clarke

and approved by

_____

_____

_____

_____

Newark, New Jersey

May 2012

Cybercrimes against the Electricity Infrastructure:
Exploring Hacker and Industry Perceptions

Abstract

The US electricity infrastructure uses Industrial Control Systems (ICS) to oversee its operations. These systems are connected online for better efficiency, making them susceptible to cyberattacks. Current research has extensively addressed ICS vulnerabilities that can be exploited by cybercriminals. Vulnerabilities, however, are only one of the many factors influencing offender decision-making in cyberattacks. Furthermore, numerous conceptions of threats, vulnerabilities, and consequences exist, which further complicate ICS security assessments. This exploratory study therefore has two main goals. First, it seeks to compare industry and hacker perceptions on electricity ICS threats, vulnerabilities, and consequences. Second, it seeks to identify a broader set of factors that influence offender decision-making in ICS cyberattacks.

Routine activity and rational choice theories guided this study. Nine preliminary offender decision-making factors were organized to create the PARE RISKS framework: Prevention Measures; Attacks and Alliances; Result; Ease of Access; Response and Recovery; Interconnectedness and Interdependencies; Security Testing, Assessments, and Audits; Knowledge, Skills, Research and Development; and System Weaknesses. A total of 323 participants from both industry and (ethical) hacking communities completed PARE RISKS surveys, which were analyzed using non-parametric statistical tests and exploratory factor analysis. Seven interviews were conducted and subjected to a thematic analysis to supplement survey findings.

The hypotheses that guided this research were all confirmed. It was found that hackers and industry experts differed in their perceptions of threats, consequences, system vulnerabilities and prevention measures. Hackers were more likely than industry respondents to believe that cybercriminals accessed hacking forums, exploited internet and email access, and exploited poor password practices. Industry respondents were more likely than hackers to believe that the desired outcomes of cyberattacks included information corruption, inaccurate information processing, and denial/disruption of service.

The PARE RISKS framework was also found to be useful in identifying factors in the pre-attack and attack-in-progress environments that influenced offender decision-making. Hackers and industry respondents believed that cybercriminals engaged in extensive research to select targets; used an assortment of techniques; operated in anonymous, compartmentalized groups; required adequate skills, money, and time; and employed cost-benefit analysis and strategic attack plans both before and during attacks.

Acknowledgements

The author recognizes the following people for their contributions in the completion of this thesis:

First of all, I was extremely privileged to have Dr. Clarke as my guru. His guidance, encouragement, commitment, and patience as I progressed through this intellectual endeavor were immensely beneficial. For all that I have learned from him, and for all his faith in me, I will forever be in his debt. I was fortunate to have Dr. Samuels as a member of my dissertation committee. He was a constant source of motivation and held a genuine interest in my success. I was also grateful to have Dr. Miller as a committee member who provided invaluable insight on the methodological aspects of this study and encouraged me to improve as a researcher. Dr. Newman, the external member of my committee, offered excellent advice and a critical eye towards my work. This project would not have been completed without the support of these mentors.

Equally responsible for my success are the 330 participants who provided the necessary data for this research. While they remain anonymous, I thank each and every one of them for making this research a success. I thank DefCon, NERC, the SANS Institute, SCADASEC, and EnergySec for providing me with the venues and means to access the research subjects.

Financially, I thank Rutgers University and the Social Science and Humanities Research Council of Canada for their generous awards and fellowships, which allowed me to concentrate fully on my dissertation.

I also thank my parents, husband, and daughter for their love, affection, and support throughout this research project. They were my cheering squad, always making me believe in myself. Were it not for their dedicated encouragement, this project would not have been possible.

Finally I thank my friends, professors, and staff at the Rutgers School of Criminal Justice for believing in my abilities and supporting me through the various stages of my research.

Table of Contents

List of Tables and Figures

Chapter I. Introduction

A nation's critical infrastructure includes those socio-economic entities that are crucial to its everyday functioning and security. Some of these include transportation, banking and finance, telecommunications, emergency services, water supply systems, and electricity systems (Blane 2002; DHS 2008; Verton 2003). The electricity infrastructure, which is the focus of this research, is an integral part of life in the United States. It is vital to industry, commercial entities, and residences. Several sources of energy can be converted to electricity; approximately 72 percent of generation in the US comes from coal and natural gas, nuclear contributes about 20 percent, while hydroelectric fluctuates between six and eight percent (EIA 2007). Renewable sources, such as wind, solar thermal and geothermal also serve as sources for electricity generation (EIA 2007).

The North American electric power sector is a very complex and networked system; it is an integrated system consisting of generation plants, high voltage transmission lines, local distribution facilities, communication, and other facilities, that operate as a synchronous network in real-time to provide stable and reliable electricity to consumers (EIA 2007). There are three power grids operating in the 48 contiguous States: (1) the Eastern Interconnected System (EIS) (for States east of the Rocky Mountains), (2) the Western Interconnected System (WIS) (from the Pacific Ocean to the Rocky Mountain States), and (3) the Texas Interconnected System (TIS) (EIA 2009). The TIS is not interconnected with the other two networks; the WIS and EIS have minimal interconnections to each other (EIA 2007). Except for Alaska and Hawaii, all US utilities

are interconnected with at least one other utility via these three major grids (EIA 2007). This interlinked system includes over 3,200 electric distribution utilities, over 10,000 generation units, tens of thousands of miles of transmission lines and distribution networks, and millions of customers (EIA 2009).

Electric utilities can be investor-owned, publicly-owned, cooperatives, and federal utilities, and are regulated by local, state, and federal authorities (EIA 2007). In 2000, transmission and distribution was valued at US$358 billion (Amin 2004). Investor-owned electric utilities are privately-owned, and operate in all states except Nebraska (EIA 2007). They represent six percent of the total electric utilities and serve about 100 million customers (EIA 2007). While investor-owned electric utilities have the fundamental objective of making a profit for their investors and are granted service monopolies, they are regulated and required to charge reasonable prices for their customers (EIA 2007). Publicly-owned electric utilities are nonprofit government entities that are organized at either the local or state level. They represent about 61 percent of the total electric utilities and account for about 15 percent of retail sales and 13 percent of revenue (EIA 2007). The cooperative electric utilities are owned by the consumers they serve. Distribution cooperatives provide retail electric service to their members, while generation and transmission cooperatives provide wholesale power and transmission service to their members. They represent about 27 percent of US electric utilities and 10 percent of sales and revenue (EIA 2007). The federal electric utility generation is primarily sold wholesale to municipal and cooperative electric utilities and to other nonprofit preference consumers. They represent less than one percent of all electric utilities and account for about one percent of total sales to consumers (EIA 2007).

Electric utilities use consumer classifications for planning and for determining their sales and revenue requirements to derive their rates (EIA 2007). Residential sectors include private households and apartment buildings, where energy is consumed primarily for space and water heating, air conditioning and refrigeration, lighting and other appliances. The industrial sector includes manufacturing, construction, mining, agriculture, fishing, and forestry establishments. The commercial sector includes nonmanufacturing establishments, such as hotels, restaurants, retail stores, health, social, educational institutions, and government (EIA 2007).

The North American electricity infrastructure has long been recognized as having problems that stem from multiple sources, such as natural disasters, system reliability, communication systems, and human error (Amin 2004). With regards to reliability issues, data from the North American Electric Reliability Corporation (NERC) and Electric Power Research Institute (EPRI) suggest that average outages from 1984 to 2004 affected nearly 700,000 customers per event annually (Amin 2004). Small-scale outages occur much more frequently and affect several thousands of customers every few weeks or months, large-scale outages occur every two to nine years and affect millions of people, and much larger outages affect seven million or more customers per event each decade (Amin 2004). Power systems need excellent communication systems, such as "high-speed data transfer among control centers to interpretation of intermittent signals from remote sensors" (Amin 2004). These internet communication systems, however, are highly vulnerable to interception and remote control. Another important source of problem is the human element. Humans interact with these infrastructures via their roles of managers, operators, and users; human performance plays a crucial role in their

efficiency and security (Amin 2004). Operators and maintenance personnel are 'inside' these networks and can have direct, real-time effects on them, often unknowingly and without malicious intent (Amin 2004).

Over the years, the electricity infrastructure has started relying on information and communication technologies (ICTs) for better efficiency and reliability (Blane 2002; Rossignol 2001; WSCCCSWG 2008; Fogarty 2011). This newly emerging, yet poorly protected, networked infrastructure invites new forms of disruption, namely cybercrime. This research defines cybercrime as any crime (i) where ICTs may be the facilitator/instrument, the victim/target of the crime, incidental to the crime, or associated with the prevalence of computers, and (ii) which may either be a single event or an ongoing series of events (Rege-Patwardhan 2009; Smith et al. 2004; Symantec 2007; Taylor et al. 2006). This definition is useful because it encompasses both the duration of the crime as well as the roles (perpetrator, facilitator, and victim) of ICTs in cybercrimes, which covers an assortment of cyberattacks that will be examined in this research.

A recent report on cybercrimes against critical infrastructure businesses found that 2,719 businesses surveyed detected 13 million incidents, suffered $288 million in monetary losses, and experienced 152,200 hours of system downtime in 2005 alone (Rantala 2008). A 2008 survey of infrastructure industry representatives conducted by Energy Insights found that the utilities infrastructure (electric, gas, and water) was the worst prepared for cyberattacks, considered to be the most vulnerable target, and to have the most detrimental consequences (GAO 2005; Nicholson 2008). An EPRI assessment developed in response to the September 11, 2001 attacks highlights three different kinds of potential threats to the US electricity infrastructure. First are attacks *by* the power

system, where the ultimate target is the population, using parts of the electricity sector as a weapon (Amin 2004). Second are attacks *through* the power system, where the utility networks serve as multiple conduits for attack, such as lines, pipes, and underground cables (Amin 2004). Finally there are attacks *upon* the power system, which is the focus of this study, where the electricity sector itself is the target. Cyberattacks against electricity sector ICS may compromise, alter, and/or steal sensitive information, cause economic loss due to reduced commercial and industrial production, disrupt the delivery of vital human services in the US, threaten public health and the environment, and possibly cause loss of human life (Copeland & Cody 2006; Blane 2002; Fogarty 2011; EIA 2007).

In addition to being a very important infrastructure, the electricity sector serves as the backbone for several other infrastructures. For instance, banking and finance depend on the robustness of electric power and wireless communications. Transportation systems rely on communication and energy networks. The link between electricity grids, telecommunications, and oil, water and gas pipelines continues to increase (Amin 2004). Indeed, electricity infrastructures are prime targets of cybercrimes and warrant special attention because incapacitating them can have a debilitating impact on everyday functionality and national security.

Research Significance, Goals, and Questions

A considerable amount of research has been undertaken on ICS security. Research areas include descriptive accounts of ICS (Ezell 1998; Luiijf 2008; DPS Telecom 2011b), ICS functionality in the electricity sector (Stouffer et al. 2011; scadasystems.net 2011),

ICS threats, vulnerabilities, consequences, and risks (SANS 2011a; Oman et al. 2001; Lemos 2000; Poulsen 2003; Luiijf 2008; Nicholson 2008), electricity sector disruption simulations (GAO 2003), and case studies (NSTAC 2000; Morain 2001; ZDNN 2001; Kuvshinkova 2003). This literature, while important, is limited to industry and security sectors, or media accounts, and is therefore technical or sensationalized (respectively) in nature. Furthermore, the studies on critical infrastructure and cybercrime are found in isolation; this disconnect hinders a thorough understanding of electricity sector cyberattacks. Finally, existing research has minimally addressed the human component in cybercrimes, specifically the factors that influence offender decision-making.

It is crucial to comprehend how offenders make decisions on target selection, exploit their criminal environment, plan, design, and execute attacks, and manage preventative and reactive measures. Using this alternate, offender-centric approach offers two benefits. First, when used in *conjunction* with the current ICS-centric approach, it may offer a more plausible and thorough set of target-based factors, such as system vulnerabilities and intrusion detection, each of which can better inform ICS security and cybercrime prevention protocols. Second, it moves *beyond* target-based factors, and focuses on the offender-related factors, such as social engineering tactics (tricking industry insiders into divulging sensitive information) and attack techniques. These factors can also help design prevention and response strategies, such as educating insiders on cross-checking the authenticity of outsiders seeking sensitive information, and tailoring prevention measures for specific cyberattacks.

This exploratory study has two main goals. First, it seeks to identify any gaps in industry and hacker perceptions on electricity sector threats, vulnerabilities, and

consequences (TVCs) as they pertain to ICS cyberattacks, and why these gaps exist. Understanding the nature and extent of these differences may help in improving or introducing technical cybercrime prevention measures, and designing appropriate administrative or educational programs. Second, this research seeks to identify the factors that may influence offender decision-making in a cyberattack. Specifically, it examines features that are inherent to the ICS being targeted (design flaws, poor prevention practices) and those that are external to the system, or, offender-specific (resources, skills). Both system- and offender-specific factors ultimately shape offender decision-making processes involved in ICS cyberattacks, which may assist industry in profiling threat agents and attack vectors, thereby appropriately blocking opportunities for cybercrime. Ten research questions drive this study:

1. How do cybercriminals select suitable ICS targets?
2. What techniques do cybercriminals use to implement ICS attacks?
3. Do cybercriminals form alliances for ICS cyberattacks? What is the nature of these alliances?
4. If alliances between cybercriminals exist, is there a division of labor?
5. What types of resources are available to offenders? How do the availability and quality of these resources impact the attack process?
6. What are the possible consequences of an ICS cyberattack?
7. Which institutions respond to ICS cyberattacks? What are some response strategies?
8. How do cybercriminals handle industry responses and evade detection?
9. What are the pre-attack factors that influence offender decision-making?
10. What are the attack-in-progress factors that influence offender decision-making?

Thesis Structure

This thesis is organized into six chapters. The next chapter introduces the theoretical framework that guides this study in understanding offender decision-making. First, Routine Activities Theory (RAT) is used, which states that three elements must converge in space and time for crime to occur, namely a capable or likely offender, a suitable target, and the absence of a capable guardian. Second, Rational Choice Theory (RCT) is used, which emphasizes the cost-benefit analysis involved in committing a crime. Both these theories focus on the situational determinants of crime and the need for crime-specific explanation, which fit with the goals of this study. These theories are used to generate five research hypotheses.

Chapter III outlines the literature review, which is conducted on five themes. First, the literature on cyberspace and its unique properties is identified. Second, research on the electricity sector and ICS is examined. ICS vulnerabilities and threats form the third and fourth themes of the literature review respectively. Electricity sector cybercrime cases comprise the fifth theme of the literature review. The theoretical framework is used to filter out relevant TVC offender decision-making factors from the literature, which are accounted for by the acronym PARE RISKS: Prevention measures; Attacks and alliances; Result; Ease of access; Response and recovery; Interconnectedness and interdependencies; Security testing, assessments, and audits; Knowledge, skills, research and development; and System weaknesses.

The purpose of chapter IV is to explain the methods that address the research questions and hypotheses. This study uses method triangulation and employs both quantitative and qualitative methods. It discusses the use of surveys, the justification for

this method, units of analysis and sampling strategies, the operationalization of PARE RISKS, and design and implementation process. It also discusses the second method of interviews, outlining its justification, sampling strategies, design, implementation, and transcription procedures.

Chapter V presents the analytical strategies for both surveys and interviews. It presents the results for all five hypotheses. The extent of the difference between hacker and industry perceptions is discussed. Non-parametric statistical tests are used to identify any differences in hacker and industry survey responses and the interviews are subjected to a thematic analysis to reveal reasons for perception gaps. The factors that influence offender decision-making are identified using both exploratory factor analysis for surveys and thematic analysis for interviews. Finally, the strengths and limitations of surveys and interviews are addressed.

The last chapter discusses some unexpected, yet important findings that emerge from this study. First, this research finds that the offender decision-making factors (PARE RISKS) are interactive resulting in attack-response cycle. Second, this research reveals a step-by-step cybercrime process with five distinct stages: preparation, entry, initiation, attack dynamics, and exit. These findings have several implications for RAT and RCT and the case is made for supplementing this theoretical framework with game theory. It also suggests practical implications, such as developing a concise set of TVC definitions that would be uniformly used and practiced throughout the electricity industry; designing educational programs for non-technical electricity sector representatives; introducing mandatory security budgets for both energy companies and ICS vendors; implementing effective sanctions for not complying with security standards;

and increasing the expertise diversity in understanding cyberattacks. The chapter also makes several recommendations for future research, such as further examining offender decision-making factors; extensively developing game theory to comprehend the dynamics of cyberattacks and industry responses; identifying the interactive nature of offender decision-making factors; developing ICS cybercrime scripts; and employing situational crime prevention measures to protect ICS from cyberattacks.

Chapter II. Theoretical Framework

Introduction

This chapter examines crime-specific theories, which form the basis of the theoretical framework for this study. First, it discusses Routine Activity Theory (RAT), which identifies three elements needed for crime to occur: capable offender, suitable target, and the absence of a capable guardian. It also addresses the importance of spatial and temporal aspects of crime, and justifies RAT's relevance to this study. The second section describes Rational Choice Theory (RCT), which views offenders as rational individuals who weigh the pros and cons of their actions. It also addresses RCT's basic premises, decision-making processes, and applications to this research. Third, a brief discussion on the complementary nature of these two theories is offered. This theoretical framework is used to develop five research hypotheses. This chapter concludes by making the case for a focused literature review using this theoretical framework.

Routine Activity Theory

Routine Activity Theory (RAT) focuses on the essential elements that constitute a crime. RAT states that three conditions must be met for crime to occur: (i) a likely or capable offender, (ii) a suitable target, and (iii) the absence of a capable guardian (Cohen & Felson 1979). Unlike many criminological theories that try to explain criminal behavior, RAT does not account for offender motivation or preexisting conditions that predispose individuals to criminality. It is not a theory of criminality, but is a theory of crime. RAT assumes that individuals have the potential to become offenders, and crime

only occurs when the likely offender comes into contact with a suitable target and there is no capable guardian to prevent this contact from occurring.

Likely offenders are any individuals who might commit a crime for any reason. The offender's assessment of the situation and/or environment determines whether a crime will take place. A suitable target can either be a person, an object, or a place, that is likely to be taken or attacked by the offender. While there are several targets, not all are suitable. To select a target, offenders will examine its location, habits, behaviors, lifestyle, living condition, and social interactions. Capable guardians are people or objects that serve to deter criminal activity; the likelihood of an attack is greater when capable guardians are lacking or non-existent. Capable guardians could be formal and deliberate (security guards), or informal and inadvertent (neighbors). Altering any or all of these elements will contribute to crime prevention or reduction.

RAT views crime from an offender's perspective; the moment an offender finds a target in the absence of a capable guardian, crime may occur. While the spatial aspect of these three elements is one aspect of RAT, the temporal aspect is also relevant. The timing of different activities by hours, days, and/or weeks are important in understanding when crime may occur. RAT recognizes that offender characteristics alone are not sufficient to account for crime; environmental factors are also relevant. Patterns of criminal behavior vary from place to place and across different time periods. When the three elements of the likely offender, suitable target, and absence of capable guardian converge in space and time, crime is likely to occur. Thus, it is important to jointly consider specific points in time and space, as well as "changes from moment to moment and hour to hour in where people are, what they are doing, and what happens to them as a

result" (Clarke & Felson 2008). Ultimately, the distribution of offenses across time and space will be a by-product of the intersection between the routine activities of both targets and offenders.

RAT is relevant to this research because it addresses the elements necessary for cybercrimes to occur in the electricity sector. The potential offenders are cybercriminals, who range in their capabilities (professional versus amateur cybercriminals). Poorly designed ICS are suitable targets, and weak real-time intrusion detection systems serve as the absence of capable guardianship. When each of these three elements coincide in space and time, ICS cyberattacks are more likely to occur. Thus, it focuses on the cybercrime event and also on the offender's analysis of the situation, which ties directly to the goals of this study.

Rational Choice Theory

While RAT is useful for examining the conditions that result in the occurrence of a crime, it needs to be complemented with rational choice theory (RCT), which views criminality as an outcome of the continual interaction between a criminal's desires and preferences, and the opportunities and constraints to commit crime (Cornish & Clarke 2008). RCT emphasizes the role of opportunity, situational factors, choices and decisions throughout the process of offending. Committing a crime, according to RCT, is seen as a series of decisions and processes made by the offender in the commission of that crime. According to RCT, an individual commits a crime because that person makes a rational choice to do so by weighing the risks and benefits of committing an act before its commission. If the risks (apprehension and punishment) outweigh the benefits then the

person will not commit the act. RCT therefore portrays offenders as active decision makers who perform a cost-benefit analysis of presenting crime opportunities; offenders are reasoning criminals who use cues from the potential crime environment in deciding whether to commit crimes, and how best to commit them (Cornish & Clarke 2008). Decision-making is constrained to certain environmental or 'situational' factors, such as time, cognitive capacity, and available information, resulting in a 'limited' or 'bounded' rationality rather than complete or perfect rationality (Cornish & Clarke 2008).

RCT has three main premises. First, it views crime as purposive behavior that is designed to meet the offender's needs (money, status), and that fulfilling these needs involves making (rudimentary) decisions and choices, which are constrained by limits of time, ability, and availability of pertinent information (Clarke & Felson 2008). Second, explaining criminal choices requires a crime-specific focus. The situational context in which decisions are made vary from one offense to another (Clarke & Felson 2008; Cornish & Clarke 2008). Offenders carry out specific crimes, each of which has its own particular motives, purposes, and benefits. Because crimes differ from each other, the factors weighed in making decisions for each crime differ substantially with respect to the nature of the offense. Thus, crime specificity in understanding offender decision-making is essential. Third, the decision-making approach should distinguish between criminal involvement and criminal events. The former refers to the processes through which individuals decide to become involved in, continue with, and desist from crime; these are multistage and extend over longer time frames. The decisions involved in each of these three involvement stages are influenced by different set of factors. The latter, criminal event, has its own set of decision processes involved in the commission of a

particular crime. The decision-making processes involved in the execution of crimes are often shorter processes that are influenced by the immediate situational settings (Clarke & Felson 2008).

This theoretical perspective is useful for capturing offender decision-making, how they decide which ICS to target, what technical attack they should use, and whether the countermeasures and security features set forth by the industry are strong enough to deter their decision to execute the attack. For example, when weighing the costs and benefits of conducting the attack, cybercriminals calculate the costs in terms of preventative measures (well-established attack countermeasures, security testing, assessments, and audits), reactive measures (quick response to, and recovery from, cyberattacks), and benefits in terms of weak system designs (easy access and built-in ICS weaknesses), which collectively determine whether the attack will occur. Furthermore, cybercriminals operate based on bounded rationality; they may not be aware of the latest countermeasures, security fixes, and attack response adequacy. As such, they may choose a strategy that they believe is effective, but may not be useful in reality. Cybercriminals tend to concentrate on only those situational factors that hinder or advance their attacks on ICS. Thus, RCT addresses offender decision-making in ICS cyberattack events, which fits nicely with the scope and goals of this study.

Combining Routine Activity Theory and Rational Choice Theory

Both RAT and RCT place importance on the situational determinants of crime, recognize the crucial distinction between criminality and crime, the need for crime-focused explanation, and organizing perspectives within which to analyze crime (Clarke

& Felson 2008). Therefore, RAT dovetails nicely with RCT, and there are two advantages to combining them. First, RAT's necessary elements for crime to occur (likely offender, suitable target, and absence of capable guardian) influence the offender decision-making processes. For instance, the capable offender may view an architecturally flawed ICS as a suitable target and poor prevention measures as the absence of a capable guardian. The likely offender may then engage in a cost-benefit analysis and decide that the pros outweigh the cons, and commit the crime. Alternatively, the situational context may present an unanticipated prevention measure (bounded rationality), which changes the cost-benefit equation, and the likely offender will not commit the crime. Thus, the three RAT elements shape decision-making of criminals.

Second, the three RAT elements are linked, such that changing any one of the elements immediately changes the likelihood that crime will occur. For instance, if an ICS improves or introduces certain prevention measures, the target may no longer be suitable to the capable offender, and a potential attack may be averted. Improving target suitability, introducing a capable guardian, and/or making an attacker incapable (bounded rationality) directly impacts the cybercriminal decision-making process. Thus, changing the RAT equation effectively alters the situational environment in which the offender operates and makes cost-benefit analysis; the *dynamic* nature of the decision-making model put forth by RCT is influenced by fluctuating RAT elements.

Research Hypotheses

This study has five hypotheses that are informed by RAT and RCT. The first three are related to the first goal of this study, which is to identify gaps in hacker and industry

perceptions of Threats, Vulnerabilities, and Consequences (TVCs), and why these gaps exist. The last two hypotheses are related to the second goal of this study, which seeks to identify factors that influence offender decision-making.

Hypothesis 1: Hackers and industry experts differ in their perceptions of threats: The different notions of threat agents, and their knowledge base, alliances, and strategies used to target ICS, may aid in understanding the likely offender, which is one element of RAT. This, in turn, can help design focused prevention measures, which impacts the cost-benefit analysis (RCT) conducted by the capable cybercriminal.

Hypothesis 2: Hackers and industry experts differ in their perceptions of consequences: The different notions of consequences, such as denial or disruption of service, may shed light on potential goals of the cyberattack or 'rewards' for cybercriminals. Even if the attack were to succeed, using system backups and alternate means to maintain functionality would render the offender's attack trivial, which would in turn, reduce/eliminate the offender's desire and efforts to target ICS. Thus, this would directly impact the capable offender's (RAT) decision making process (RCT).

Hypothesis 3: Hackers and industry experts differ in their perceptions of system vulnerabilities and prevention measures: The different notions of system weaknesses, such as architectural flaws and poor password practices, may aid in understanding the suitable target, which is the second element of RAT. The prevention measures, such as intrusion detection systems and anti-virus software serve as the capable guardian of ICS, which is the third element of RAT. While these measures serve to guard ICS from cyberattacks, they may not be 'capable'. Understanding what makes a target 'suitable'

and a guardian 'capable' may help industry redirect or improve prevention measures to better safeguard ICS, thereby increasing the costs undertaken by the offender (RCT).

Hypothesis 4: The factors in the pre-attack environment that impact offender decision-making processes include prevention measures, alliances, result, accessibility, security testing, target reconnaissance, and exploitable weaknesses: According to RAT, crime occurs when a potential offender, suitable target, and an incapable guardian coincide in space and time. Hackers identify suitable targets based on their accessibility, and system weaknesses. Additionally, hackers detect the lack of a capable guardian based on preventative measures. RCT states that these system opportunities, such as poor prevention measures, and constraints, such as unexpected preventative measures impact cybercriminal decision-making in ICS cyberattacks. Thus, the pre-attack environment, which involves the suitable target and the absence of a capable guardian, will impact the cost-benefit analysis that the potential offender engages in. Therefore, understanding this pre-attack environment and the factors that influence the offender decision-making process are crucial to the industry in designing the appropriate prevention at ICS entry points.

Hypothesis 5: The factors that impact offender decision-making processes also emerge from the attack-in-progress environment, and include attack techniques, target responses, and exploitable weaknesses: Merely infiltrating the system does not guarantee a successful attack, as the industry may detect and respond to an attack upon its inception. The three elements of RAT (likely offender, suitable target, and the absence of a capable guardian) may not be static once the attack commences. For instance, an unanticipated industry response may suggest that a capable guardian is present, which makes the target

unsuitable and deters the capable offender. That is, the potential offender may engage in a cost-benefit analysis as the crime progresses. Thus, pre-attack peripheral prevention measures should be coupled with both internal prevention measures and reactive measures to generate the strongest and most successful defense mechanisms, which would deter the capable offender by increasing the costs involved in continuing with the attack.

Conclusion

This chapter addressed routine activities theory (RAT) and rational choice theory (RCT), which were combined to create a theoretical framework that accounted for offender decision-making in ICS cyberattacks. It also developed five hypotheses to identify perception differences and decision-making factors.

To test these hypotheses, however, it is important to identify the relevant elements of RAT and RCT as they pertain to ICS cyberattacks in the existing literature. As such, the following questions arise: What makes an ICS suitable for cyberattacks? What preventative measures are being used to protect ICS? What/who are the capable offenders that target ICS? How do capable offenders decide which ICS to target? What factors inherent to ICS affect the offender decision-making process? What offender-specific factors influence decision-making processes? In order to answer these questions, the next chapter reviews the existing ICS literature to identify industry conceptions of ICS threats, vulnerabilities, and consequences, the structure and components of ICS, and ICS cybercrime case studies to identify factors that influence the decision-making process of offenders.

Chapter III. Literature Review & PARE RISKS Framework

This chapter conducts a focused literature review, which is informed by the theoretical framework discussed in the preceding chapter. Five themes of literature are reviewed. First, the literature on cyberspace and its unique properties that facilitate cybercrime is examined. Second, electricity ICS literature is reviewed, which provides information on ICS components, their functions, and inter-relationships that can be targeted by cybercriminals. Third, the literature on ICS vulnerabilities is examined, which offers insight into system design or architecture flaws that make them suitable targets. Fourth, the literature on ICS threats is reviewed, which identifies the assortment of cybercriminals based on types and skills. Finally, twelve case studies of cybercrimes against the electricity sector are listed to illustrate the varying nature, diversity, and intensity of strategies and cybercriminal skills. Following this literature review, definitions are offered for the concepts of threats, vulnerabilities, and consequences as they pertain to this research. Finally, the factors that influence offender cost-benefit analysis are extracted from the literature review and combined to create a nine-factor PARE RISKS offender decision-making framework.

Technology and Cyberspace

The literature on technology and cyberspace suggests five themes. The first theme found in the literature is globalization. Faster and larger information flow in networked societies has resulted in homogenization; some researchers suggest that the proliferation of information and communication technologies (ICTs) will result in one culture, with all

individuals living, thinking, and acting in similar ways (Ritzer 1996; Barber 1995; Newman & Clarke 2003). Block (2004) claims that the internet has two important functions: (i) it enables the publication and dissemination of information without direct contact, and (ii) it operates as an international marketplace which is proliferating rapidly. Other researchers examine the impacts of globalization and technology on the economy, suggesting that developing and underdeveloped nations face a disadvantage in the competitive world marketplace because they are technologically laggard (Siddiqui 1998; Kellner 2001; Archibugi & Pietrobelli 2003).

Second, the literature identifies the theme of virtual communities. Oldenburg (1989) suggests that individuals move through three environments, where they work, live, and meet others for social bonding. In contemporary societies, where individuals experience only two environments (work and home), Oldenburg (1989) argues that individuals often feel abandoned and isolated. Hence, they turn to the internet to experience bonding and closeness, thereby re-establishing the third environment. Rheingold (1993) agrees with Oldenburg (1989), suggesting that virtual communities have burgeoned due to individuals' search for social companionship. Rheingold (1993) argues that online communities have proliferated due to the excitement internet users experience by interacting with other people through a new, digital medium. He identifies the unique traits of online relationship, such as the lack of face-to-face contact, the lack of spatial-temporal constraints, and the use of computers for communication. Jones (1995), Oldenburg (1989), Rheingold (1993), and Rege (2009) claim that the ability to interact, gain new information, and develop relationships have made online communities popular among individuals seeking to re-create a sense of community and social bonds.

Alternatively, Ludlow (1996) argues that online communities also alienate individuals and contribute to the loss of community in the real world. However, he argues that virtual communities can recreate the sense of community and bonding that are no longer limited by geography, but are created through common interests.

The third theme found in the literature involves notions of identity in cyberspace. Reid (1994) argues that M.U.Ds (Multi User Dungeons), a virtual community for online games, offer a playground for the self; an environment where individuals can test different ways of being. She argues that the combined effect of anonymity, distance, and flexibility offered by ICTs imply that players are not fixed entities in the MUD environment; their online manifestation is alterable and open to (re)interpretation. Turkle (1997) agrees with Reid (1994) and argues that identity is no longer singular, but multiple. Individuals create several different identities based on their creativity and imagination, which in turn blurs the boundaries between real and virtual (simulated) identities (Turkle 1997). Poster (1995) claims that multiple identities in cyberspace are created external to the individual. He suggests that analogous to the real world, which creates subjectivity, cyberspace is a (virtual) reality that constitutes subjects. Poster (1995) claims that in the virtual world, detailed information about individuals is stored in databases in an assortment of categories, such as age and gender. This information 'interpellates' the subject, i.e., these categories become new additional online identities that are used to constitute individuals. The internet enables the manipulation and reinvention of social identity; individuals can adopt multiple new online personae that are potentially far removed from their 'real world' identities (Yar 2006, Rege 2009).

Surveillance in cyberspace is the fourth theme recognized in the literature. Lyon (1994) notes that in the surveillance society, details of individuals' lives are collected, stored, categorized, retrieved, and processed by complex computer systems owned by governments and corporations. Like Poster (1995), he suggests that this sophisticated surveillance enables the integration of data, which forms an individual's 'data image'. This data image is a complex combination of diverse bits of data, which influence the decisions and judgments made about that corresponding individual (Lyon 1994). Whitaker (1999) and Staples (2000) also note that surveillance is used as a mechanism of power. They argue that power in the networked world is no longer centralized. New decentered surveillance technologies make individuals' lives transparent, i.e., they can no longer elude surveillance systems. Haggerty and Ericson (2000) argue that ICTs have enabled a surveillant assemblage, which has changed the purposes and hierarchies of surveillance. These surveillant assemblages are composed of discrete flows of limitless information such as "people, signs, chemicals, knowledge, and institutions" (Haggerty & Ericson 2000, p. 608). Like Whitaker (1999) and Staples (2000), they argue that this assemblage has resulted in the 'disappearance of disappearance' – a stage where it is increasingly difficult to remain anonymous.

The fifth theme in the literature identifies the characteristics of cyberspace. The internet enhances the potential for criminal and deviant activities to occur in several important ways. First, there is a tremendous growth in the number of people with internet access. The potential victim base is estimated to a little over six billion (and continually rising), which provides limitless opportunities for cybercriminals (Internetworldstats.com 2010; Jewkes 2003). Second, the degree of anonymity offered by cyberspace offers a

lower risk of detection than other crimes (Jaishankar 2009; Jewkes 2003, Rege 2009). Third, cyberspace also reconfigures time and space, so that offenses can be initiated, and their impact felt, worldwide (Jewkes 2003; Smith et al. 2004; Yar 2006). Fourth, ICTs enable a single individual to reach, interact with, and affect thousands of individuals simultaneously; technology therefore acts as a 'force multiplier', enabling individuals with minimal resources to generate potentially huge negative impacts (Jaishankar 2009; Yar 2006). Fifth, velocity is an important characteristic of cybercrime; viruses can spread worldwide at 'hyper-speed', and cyberattacks can cripple victims instantaneously (Jaishankar 2009). These novel social-interactional features of cyberspace, such as the collapse of spatial-temporal constraints, the one-to-many and many-to-many connectivity, the anonymity and changeability of online identity, and velocity of the crime, make possible new forms and patterns of illicit activity. Newman and Clarke (2003) capture these criminogenic traits of cyberspace through their acronym SCAREM: Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity. Cybercriminals are invisible and anonymous in cyberspace, difficult to detect, and rationally choose their targets, and can easily replicate their crimes.

This literature review raises several questions that are relevant to this research. How do notions of identity and anonymity aid in the commission of cybercrimes against electricity ICS? Is information about ICS vulnerabilities readily available online via virtual communities? How do electricity ICS benefit from the properties of ICTs and cyberspace? To address these questions, the literature on electricity sector ICS was examined.

Electricity Infrastructure and Industrial Control Systems

The electricity sector uses Industrial Control Systems (ICS), which is a general term that encompasses several types of control systems, including Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Supervisory Control and Data Acquisition (SCADA) systems (Stouffer et al. 2011; WSCCCSWG 2008). SCADA systems are highly distributed systems, which are used to control geographically dispersed assets, often scattered over vast distances, where centralized data acquisition and control are critical to system operation (Stouffer et al. 2011). Both the electrical power transmission and distribution grid industries use SCADA systems to monitor and control electricity distribution (Stouffer et al. 2011). SCADA systems are designed to collect field data, transfer it to a central computer facility, and display this data to the plant operator graphically or textually, thereby allowing the operator to monitor or regulate an entire system from the central location in real time (Stouffer at al. 2011). SCADA systems control *and* monitor processes, which can be infrastructure, facility, or industry based. The infrastructure processes can be private or public and includes electrical power distribution and transmission (scadasystems.net 2011). Facilities, such as airports, ships, and buildings have facility processes, which control and monitor access and consumption (scadasystems.net 2011). Industrial processes include "production, refining, manufacturing, fabrication, and power generation and may run in batch, continuous, discrete or repetitive modes" (scadasystems.net 2011).

A DCS is responsible for controlling production systems within the same geographic locations for industries, such as electric power generation plants and oil refineries (Stouffer et al. 2011). There is often confusion over the differences between

SCADA and DCS. SCADA systems, as the acronym implies, includes data acquisition *and* control, while DCS is purely control oriented (DPS Telecom 2011b). Before the introduction of computer networks, a SCADA system was the top-level controller for lower-level systems as it was impractical for SCADA to control every minute aspect of a system (DPS Telecom 2011b). Here, DCS did most of the lower level detail work and reported back to, and took orders from, the SCADA system (DPS Telecom 2011b). With the growth of fast computer systems, however, SCADA and DCS have blurred together into a single monitoring and control system (DPS Telecom 2011b).

PLCs are control systems that are typically used throughout SCADA and DCS systems to provide local management of processes (Stouffer et al. 2011). Data acquisition starts at the PLC level, which includes equipment status reports and meter readings, which are then communicated to the SCADA system (scadasystems.net 2011). Based on the data collected from the stations, automated or operator-driven supervisory commands are sent back to the PLCs, which in turn control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions (Stouffer et al. 2011).

While ICS used in distribution and manufacturing are very similar in operation, they are different is some characteristics. First, DCS or PLC-controlled subsystems are usually located within a more confined area, while SCADA systems are geographically dispersed (Stouffer et al. 2011). Second, DCS and PLC use high speed communications, while SCADA systems employ long-distance communication systems (Stouffer et al. 2011).

Most ICS in use today were developed years before public and private networks or the internet were commonplace in business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements (Stouffer et al. 2011). They were physically isolated from outside networks and based on proprietary software, hardware, and communication protocols that included basic error identification and correction capabilities, but lacked the secure communication capabilities needed in today's interconnected systems (Stouffer et al. 2011). Information and communication technologies (ICTs) started making their way into ICS designs in the late 1990s, exposing them to new types of threats and significantly increasing their vulnerability (Stouffer et al. 2011).

The US critical infrastructure is highly interconnected and mutually dependent through a host of ICTs; an incident in one infrastructure can directly, or indirectly, impact other infrastructures through cascading and escalating failures (Stouffer et al. 2011). Electric power is often considered to be one of the most prevalent sources of disruptions and cascading failures of interdependent critical infrastructures. A disruption in the electricity sector could result in large area blackouts that could impact oil and natural gas production, water treatment systems, wastewater collection systems, and transportation systems that rely on the grid for power (Stouffer et al. 2011).

Disruptions in the electricity sector have been simulated. For instance, ICS researchers at the Department of Energy's national laboratories demonstrated the feasibility of cyberattacks on electric power substation ICS (GAO 2003). Using tools that were readily available online, they modified data from field sensors and took control of the PLC directly, allowing them to change settings and create new output (GAO 2003).

These techniques could easily enable cybercriminals to incapacitate the substation and cause an outage.

While this literature identifies the different types of ICS and their uses in the electricity sector, it does not shed light on their vulnerabilities. As such, this research examines the following questions: What types of vulnerabilities are present in ICS? Are these vulnerabilities inherent to system architecture or network flaws? To address these questions, the literature on ICS vulnerabilities was reviewed.

Industrial Control System Vulnerabilities

Several overlapping definitions of vulnerabilities are found in the literature. Vulnerabilities are any weaknesses that can be exploited by an adversary to gain access to an asset (Byres & Lowe 2004). Haimes (2006) defines a vulnerability as the manifestation of the inherent states of the system (physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system. Another definition of vulnerability is a weakness that can be exploited to gain access to a given asset and subsequent destruction or theft of the asset (as cited in Moteff 2005, p.7). Vulnerabilities have also been defined as the "characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result to having been subjected to a certain level of threat" (Robles et al. 2008). The DHS (Department of Homeland Security) Risk Lexicon (2010) defines vulnerability as a physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.

ICS have several built-in vulnerabilities, which made them suitable targets. ICS were designed and implemented in an era when network trespass and data manipulation were not relevant. Information security was not built-into these systems because there was "no public information on how SCADA worked, … no connections to the [internet], … the environment was assumed to be hacker-free, [and that the systems operated in] totally controlled and closed secure environments" (Luiijf 2008, p. 11; Nicholson 2008; Stamp et al. 2003). However, the increasing use of cost-cutting ICTs, which offered convenience and efficiency, also increased the likelihood of ICS cyberattacks.

The National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems Security categorizes ICS vulnerabilities into three groups: Policy and Procedure, Platform, and Network categories. There is no pecking order of vulnerabilities with regards to the likelihood of occurrence or severity of impact (Stouffer et al 2011). Policy and procedure vulnerabilities are often introduced into ICS because of incomplete, inappropriate, or nonexistent security policy documentation. This documentation identifies safe user practices, such as regular password updates, and network connection requirements (Stouffer et al 2011). The lack or paucity of security audits is also problematic as this process typically determines the adequacy of system controls and ensures compliance standards are met (Stouffer et al 2011). There is no consistent use of tools such as "end-to-end threat-vulnerability-consequence analysis and evaluation of cyberattack and response simulators", nor is there a regular adoption of industry-approved incident reporting protocols and recommended practices (WSCCCSWG 2008, p. 27; Public Citizen 2004). While incomplete and nonexistent documentation is one part of the problem, the other relates to the easily available ICS information and

resources (Stouffer et. al. 2011; Luiijf 2008). In the electricity sector, open sources of information, such as "product data and educational videotapes from engineering associations", can be utilized by anyone to understand the basics of the electrical grid (GAO 2003, p. 13). ICS vendors are publishing their proprietary protocols and specifications to enable third-party manufacturers to build compatible accessories (Stouffer et al. 2011). Other publicly available information, such as Federal Energy Regulatory Commission (FERC) reports, industry publications, maps, and material available online, is sufficient to allow cybercriminals to identify the most heavily loaded transmission lines and the most critical electricity substations (GAO 2003). Furthermore, SCADA tutorials are easily available online as downloadable white papers, YouTube videos, and 'ask SCADA experts' websites (DPS Telecom 2011a; YouTube 2009; Zintro 2011). SCADA systems run as Windows or Linux applications, whose vulnerabilities are well-known and available to hackers worldwide and can be exploited easily (Luiijf 2008). Thus, the internet serves as an extensive knowledge base documenting system blueprints and protocols, tutorials and expert advice, and vulnerability details.

Platform vulnerabilities are those ICS vulnerabilities that occur due to flaws, misconfigurations, or poor maintenance of their platforms (Stouffer et al 2011). Platform vulnerabilities further exist as four sub-groups: configuration (undeveloped operating system patches, patches implemented without exhaustive testing, no password used), hardware (insecure remote access on ICS components, lack of backup power, lack of redundancy for critical components), software (buffer overflow, denial of service, logs not maintained), and malware protection (malware protection software not installed, not current, or implemented without exhaustive testing) (Stouffer et al 2011). Human-

machine interface (HMI) of SCADA systems now utilize user-friendly browser applications that can be easily understood and employed by anyone, and thus little technical expertise is required to operate these systems (Luiijf 2008). Furthermore, organizations are transitioning from proprietary systems to less expensive, standardized technologies, such as commercial-off-the-shelf (COTS) SCADA systems and software. COTS software, however, has publicly known design errors and bugs, which be easily exploited using tools that are widely available online (Luiijf 2008; Stouffer et al. 2011).

A third source of ICS vulnerabilities occur from flaws, misconfigurations, or poor administration of ICS networks and their connections with other networks (Stouffer et al 2011). First is the network configuration vulnerability, which includes weak network security architecture, unencrypted passwords, and indefinite existence of passwords. SCADA systems are now remotely accessible for control and maintenance by plant operators (Luiijf 2008; Stouffer et al. 2011). Additionally, many organizations have added connections between corporate networks and ICS networks, which give the corporation's decision makers access to critical data and relay corresponding instructions back to the ICS (Stouffer et al. 2011). This integration of ICS networks with public and corporate networks, however, increases the accessibility of ICS and their vulnerabilities (Stouffer et al. 2011). Furthermore, network passwords are rarely changed because the SCADA environment is assumed to be secure (Luiijf 2008; Nicholson 2008). Adversaries with password cracking software can easily gain access via remote connections and obtain administrator access (Stouffer et al. 2011). Collectively, remote accessibility and bad password practices invite cyberattacks as outside parties can connect equipment to SCADA systems without supervision (Luiijf 2008). Network hardware vulnerabilities

include unsecured physical ports, non-critical personnel access to equipment and network connections, and the lack of redundancy for important networks. Network perimeters are the third type of network vulnerability, and includes the lack of security perimeter definition and nonexistent or improperly configured firewalls. Technical protection is often lacking, with virus scans rarely being performed and security patches not being installed regularly and rigorously; insufficient quality control for SCADA software, poor or improper usage of firewalls, lack of individual authentication, and poor intrusion detection collectively increase the risk of cyberattacks (Luiijf 2008; Nicholson 2008).

While this literature identifies the different types of ICS vulnerabilities, it does not identify the various types of threats faced by ICS. Cybercriminals operate in cyberspace and use ICTs to communicate and conduct their crimes. What types of attackers pose a threat to the electricity infrastructure? What expertise do they possess? What is their modus operandi? How do cybercriminals operate in these digital environments? To address these questions, the literature of ICS threats and cybercriminals was studied.

Industrial Control System Threats

There are several definitions of threats found in the literature, which share common components. Threats have been defined as any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset (Byres & Lowe 2004; Moteff 2005). An additional definition of threat is the intention and capability of an adversary to undertake actions that would be detrimental to US interests (as cited in Moteff 2005, p.7). Threat is also defined as the intent and capability to adversely affect

(cause harm or damage to) the system by changing its states (Haimes 2006). The DHS Risk Lexicon (2010) defines threat as a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Numerous sources serve as threats to ICS, which include adversarial sources, such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders, and non-malicious sources, such as system complexities and failures, human errors, and natural disasters (Stouffer et al 20110). This research focuses on the adversarial sources and for the purpose of this research, cybercriminals are offenders who (i) are driven by a range of motivations, such as thrill, revenge, and profit, (ii) commit and/or facilitate cybercrimes, (iii) work alone, in simple partnerships, or in more formalized settings, and (iv) have varying levels of technical expertise (Rege-Patwardhan 2009). In the context of this proposal, the category of cybercriminals includes insiders (current and past employees) in addition to outsiders, as they perpetrate cybercrimes against the very structures they are expected to protect. Three main themes emerge in the literature on cybercriminals.

The first theme found in the literature identifies ten threat sources to critical infrastructures. First, *leisure cybercriminals* break into networks for the thrill of the challenge or for bragging rights in the cybercriminal community (Stouffer et al. 2011). While remote cracking once required technical knowhow, leisure attackers can now download attack scripts to launch attacks against ICS, thereby increasing the possible pool of attackers (Stouffer et al. 2011). A variant of this category is the *bot-network operator* who takes over multiple systems to coordinate attacks and to disseminate

phishing schemes, spam, and malware attacks rather than engaging in system intrusions for challenge and bragging rights (Stouffer et al. 2011). Second, *industrial spies* seek to acquire intellectual property and knowhow through covert methods (Stouffer et al. 2011). Third, *foreign intelligence services*, or *nation-states*, are developing information warfare doctrines, programs, and capabilities, which can have a major impact by disrupting the supply, communications, and economic infrastructures that support ICS in several infrastructures (Stouffer et al. 2011). Fourth, *terrorists* seek to disrupt, debilitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence (Stouffer et al. 2011). Fifth, *disgruntled insiders* possess ICS knowledge and unrestricted access to cause system damage or steal sensitive information; they may be employees, contractors, or business partners (Stouffer et al. 2011). Sixth, *professional cybercriminals* have a high degree of technical acumen, access to state of the art equipment, and use their technical expertise to further their own criminal pursuits (Rogers 2005). Seventh, *criminal groups* seek to attack systems for monetary gain, and use spam, phishing, and malware to conduct their attacks; they may hire or develop cybercriminal talent to target ICS (Stouffer et al. 2011). *Phishers* are the eighth type of cybercriminals. These are individual or small groups of cybercriminals that execute online schemes, via spam, spyware, and malware, to steal identities or information for monetary gain (Stouffer et al. 2011). Ninth, *spammers* are cybercriminals that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, or distribute spyware and malware (Stouffer et al. 2011). Finally, *spyware/malware authors* are individuals or organizations with malicious

intent and carry out attacks against users by producing and disseminating spyware and malware (Stouffer et al. 2011).

Cybercriminal taxonomy based on technical expertise is the second theme found in the literature. There is a pecking order to online deviants, each with its own set of motivations and rationales. At the bottom, is the *script kiddy*, an amateur attacker who uses codes written by others to exploit the vulnerabilities in computer systems. They are generally under the age of 20, and have little knowledge about the workings of the programs. They execute but do not plan cyberattacks (McAfee 2005). Next are *cyberpunks* who have malicious intents. They use their computer skills to break into networks and systems, but they are not motivated by money. Their deviant acts typically involve website defacement, or 'cybergraffiti', which places embarrassing content on targeted websites, motivated by either revenge or a political agenda (McAfee 2005). Then there are *hackers* and *crackers*. Hackers are passionate about learning new programming languages, playing with computer systems, and have a strong sense of morals (McAfee 2005). Ethical hackers do not cause damage, and have very strict ethical guidelines concerning their work. Crackers, however, are those individuals that gain unauthorized access to computer networks. They generally operate alone and their goal is to gain a reputation in the cracker community. (McAfee 2005). *Cyber gangs* make a living out of online criminality and operate in areas with weak cybercrime laws and law enforcement. These virtual gangs usually involve loose, fluid networks of criminals located in several different countries who work in partnership for a criminal organization (McAfee 2005). *Information merchants*, for example, are part of these online gangs, and they are responsible for the profitable sale of data, engaging in crimes such as espionage,

sabotage, and computer network break-ins. Unlike crackers, information merchants are primarily driven by profit (Bednarski 2004).

Cybercriminal rationales and motivations comprise the third theme found in the literature on cybercriminals. Seven rationales have been used to explain hacking, cracking and intrusions. First, is *curiosity*; cybercriminals are curious about the operation of networks, computer viruses, and worms, and wish to learn more about them (Weaver et al. 2003). Second, is *spying*; cybercriminals wish to access personal files or monitor the activities of others for overt or covert reasons (Reuters 2006). Corporate spies can be divided into two distinct groups. Most corporate espionage is conducted by business insiders, who have legitimate access to a company's computer networks, such as employees, information technology personnel, or corporate executives. The remaining corporate espionage is done by outsiders or persons who crack into a corporation's computer data networks without any form of legitimate access rights (Taylor et al. 2006). Cybercriminals are also motivated by *thrill* and/or *challenge* (Warner 2001). They thrive on the excitement of cracking a program or server and challenge authorities by demonstrating their expertise. A fourth motivation for committing cybercrimes is *status* (Krone 2005). Cybercriminals wish to gain status in the hacking and mainstream community. Cybercriminals can also subscribe to various *political* ideologies (Weaver et al. 2003). A sixth motivation for cybercriminals is *revenge*. These cybercriminals may include disgruntled ex-employees seeking vengeance on their employers (Datz 2004). Finally, *monetary gain* is also a motive that drives cybercriminals, which can be accomplished by selling digital loot, renting out hacking services and products, or through extorting targeted sites after attacks (Krone 2005, McMullan & Rege 2007).

The preceding bodies of literature discuss ICS threats and vulnerabilities. No literature specifically focuses on the consequences of ICS cyberattacks. As such, a review of known electricity sector cyberattacks is offered to capture not only the consequences, but also the different threat agents and attack techniques and frequency.

Electricity Cyberattacks, Consequences and Vulnerability Disclosures

Twelve known and simulated ICS cyberattack cases are found in the literature, which are listed chronologically. The first two cases, however, do not have information on attack details, source, duration, or time; these cases are listed in a 2001 report and are therefore assumed to have occurred before the other ten cases. The first case noted that on several occasions, hackers targeted IT systems in the electricity sector seeking credit card information (SANS 2011a; Oman et al. 2001). In the second case, a radical environmental group was caught hacking into the IT system of an undisclosed electric utility company (SANS 2011a; Oman et al.2001). The electricity sector even experienced threats from insiders, such as employees, contractors, or anyone with legitimate access to the system. In 2000, a letter written by a disgruntled ex-employee of an unnamed electric utility in Texas appeared in the hacker magazine Phrack. The author claimed to know "quite a bit about the systems and hinted that his knowledge would be helpful if someone wanted to attack [the] utility's systems" (NSTAC 2000; SANS 2011a).

The fourth case occurred in 2000, at another unnamed power company. Here, hackers subverted the company's server to play games (SANS 2011a; Oman et al. 2001). The intruders gained access to the servers by exploiting a vulnerability in the company's file storage service (Lemos 2000). They consumed about 95 percent of the company's

internet bandwidth to store and play interactive games (Lemos 2000). The compromised bandwidth threatened the company's ability to conduct bulk power transactions, resulting in a denial of service attack on the servers' legitimate users (Lemos 2000; SANS 2011a). The hackers used an automated tool that scanned the internet for 'anonymous FTP servers' with the file storage vulnerability (Lemos 2000). As one security expert noted the incident "seems just like a bunch of kids playing… they weren't targeting the company. It just seems like one of those indiscriminate acts" (Lemos 2000, p.1). While this attack was not a serious threat that intentionally targeted the electricity sector, attackers could have placed malware into the system, which would have given them to hijack the system (Lemos 2000).

The fifth case involved the California Independent System Operator (Cal-ISO), which oversaw most of the state's massive electricity transmission grid. The attack began April 25, 2001 and remained undetected until May 11 (Morain 2001). It was routed through China Telecom from someone in the Guangdong province of China (Morain 2001). Attackers also entered the system via internet servers based in Santa Clara in Northern California and Tulsa, Oklahoma (Morain 2001). This breach was claimed to have occurred after the collision between a Chinese military jet and a US spy plane (Morain 2001). Several computer attacks occurred in the US that originated in China, and mostly involved mischief, such as anti-American slogans scrawled on US government web sites (Morain 2001). Investigators found evidence that the hackers were trying to write software that would have allowed them to bypass any firewalls protecting the more sensitive parts of the computer system (Morain 2001). They also found evidence that a

rudimentary rootkit had been installed, which would have given the attackers complete control of the system (ZDNN 2001). The attackers focused on the grid's computer system that was under development, not protected behind a firewall, and directly connected to the internet (Morain 2001; ZDNN 2001). Furthermore, Cal-ISO did not have any intrusion detection systems in place that would have alerted it to the unauthorized entry. System logs that might have identified users entering the servers as the infiltration was occurring were also non-existent (Morain 2001; ZDNN 2001). Compounding these problems was the fact that dozens of ports into the computer systems were open (Morain 2001). Investigators were limited in their ability to discover all files and activity that had actually occurred because workers at Cal-ISO rebooted their computers in response to the infiltration (Morain 2001). While one security expert stated that "there [was] no elegance to this intrusion. This [was] just a case of throwing enough mud and hitting something. A skilled hacker would have been able to hide his tracks better", this case demonstrated the ease with which Cal-ISO was targeted and how it could have had a more debilitating impact (ZDNN 2001).

The 2003 Slammer worm, which was the sixth case found in the literature, impacted the internet and many services, including some electricity sector systems (Kuvshinkova 2003). One such system was that of Ohio's Davis Besse nuclear power plant, where the Slammer work penetrated the unsecured network of an "unnamed Davis-Besse contractor, then squirmed through a T1 line bridging that network and [the company's] corporate network" (Poulsen 2003, p. 1). This connecting network completely bypassed the firewall that would have otherwise blocked the port through

which Slammer had entered (Poulsen 2003). It then went from the corporate network to the plant network, where it found an unpatched Windows server to lock on and propagate (Poulsen 2003). Even though a patch for the MS-SQL vulnerability that Slammer exploited had been released six months before Slammer's launch, plant computer engineers were not aware of it and hence had not installed it (Poulsen 2003). Slammer, which was released by an unknown source, essentially slowed down the plant network and crashed the plant's computerized display panel, called the Safety Parameter Display System (SPDS) (Poulsen 2003). An SPDS monitors critical safety indicators at a plant, such as "coolant systems, core temperature sensors, and external radiation sensors" (Poulsen 2003, p. 1). Another, less important, monitoring system called the Plant Process Computer (PPC) also crashed; it took approximately five to six hours to restore both the SPDS and PPC (Poulsen 2003). While these systems had redundant analog backups that were unaffected by the worm, their unavailability was taxing for the operators (Poulsen 2003).

The seventh case highlighted the potential for cyberattack against the US electricity grid. In 2009, cyberspies penetrated the US electrical grid and left behind malware that could be used to navigate the US electrical system and its controls (Gorman 2009). While detailed information about this case, the type of malware, and the potential damage that could occur was not released, it was noted that spies came from China, Russia, and other countries who were "on a mission to navigate the U.S. electrical system and its controls" (Gorman 2009, p.1). The espionage did not target any particular utility company or region and was pervasive across the U.S. (Gorman 2009).

The more publicized Stuxnet worm, which was the eighth case, first appeared in July 2010 and approximately 60 percent of its reported infections were inside Iran (BBC 2011). The worm targeted PLCs made by Siemens, and it was intended for those inside Iran's Bushehr nuclear facility (BBC 2011). Security experts stated that Stuxnet was used to target Iran's machinery that enriched uranium for both nuclear power and weapons (BBC 2011). While no concrete evidence exists for who created Stuxnet, several bits of evidence suggested that an Israel-US alliance may have been the source (Broad et al. 2011; BBC 2011). Experts stated the worm only kicked into gear when it detected the presence of a specific configuration of controllers, running a particular set of processes that only existed in a centrifuge plant (Broad et al. 2011). The worm was a "dual warhead" as it had two major components (Broad et al. 2011, p. 5). The first was designed to lie dormant for long periods, then sped up the machines to "send Iran's nuclear centrifuges spinning wildly out of control", leading to its eventual destruction (Broad et al. 2011, p.2). The second component, the "man in the middle", was a computer program that secretly recorded normal plant operations, then played those readings back to plant operators, "like a pre-recorded security tape in a bank heist", to make it appear that everything was operating normally, when in fact, the "centrifuges were actually tearing themselves apart" (Broad et al. 2011, p.2). As one expert noted, Stuxnet was not about sending a message or proving a concept, it was about "destroying its targets with utmost determination in military style" (Broad et al. 2011, p. 6). A 2011 report published by Symantec suggested that it would have taken a team of between five to ten core developers (not including individuals needed for quality assurance and management) roughly six months to create the worm. They must have created a "mirrored environment

that would include the necessary ICS hardware, such as PLCs, modules, and peripherals in order to test their code" (Falliere et al. 2011, p. 3).

In the ninth case, US Department of Energy labs and research facilities were targets of cybercrimes. In April 2011, the Oak Ridge National Laboratory, which conducts applied research, was forced to shut down internet and email access after an unknown system vulnerability had been exploited (Jackson 2011a). In July 2011, two energy department research facilities were taken offline by a sophisticated cyberattack (Jackson 2011a). The Pacific Northwest National Lab (PNNL) worked mostly in the areas of national and homeland security research and the Jefferson Lab dealt with nuclear physics and technology (Jackson 2011a). These labs had computers that stored intellectual property, unpublished scientific results, classified information, and other sensitive information, making them prime targets for cyberattacks (Cary 2011; PureVPN 2011). PNNL fended off approximately four million cyber-attacks a day, most of which were easy to detect and defend against, but this attack was more serious (Carey 2011; Jackson 2011b; PureVPN 2011). Company officials stated that the attacks were most likely targeting "Energy Sciences Network (ESnet), a high-speed, high-resiliency network that inter-connects major Department of Energy laboratories including Oak Ridge, PNNL, FermiLab and the Y12 National Security Complex" (PureVPN 2011). PNNL teams found malware that had been described as "Advanced Persistent Threat", a type of malicious code that was intended to "quietly infiltrate a system and operate below the radar while searching for information or waiting for instructions" (Jackson 2011b, p. 1). These attacks were well-funded and involved persistent individuals looking for

intellectual property or national security secrets (PureVPN 2011). PNNL's chief information officer noted, "it appears that no matter what we do, the attackers just have the right attack figured out already" (PureVPN 2011, p. 2).

While the above cases listed actual cyberattacks, the next set of cases demonstrated how attacks could easily be conducted. In the tenth case, an NSS Labs (security research and testing lab) researcher gave a demonstration at the 2011 Black Hat conference on how hackers could take over the Siemens S7 computers that were used to control industrial facilities (McMillan 2011). The researcher found ways to bypass the S7's security measures and read and write data onto the computer's memory, even when password protection was enabled (McMillan 2011). On one model, S7 300, he found a command shell that had been left by Siemens engineers, which he could connect to and use to run commands on the system (McMillan 2011). The S7 300 was widely used in the electricity sector (McMillan 2011). He also discovered a hard-coded username and password "username: basisk; password: basisk" that allowed him access to a "Unix-like shell program on the systems, where he [could] run his own commands" (McMillan 2011, p. 1) These shell programs served as a 'back door' to the systems that could easily be exploited by attackers.

The other demonstration on ICS vulnerabilities, the eleventh case, also occurred at Black Hat, which demonstrated that plant operators sometimes "practically advertise[d] their wares on Google Search… That's like putting up a billboard saying SCADA... system here, and oh by the way, here are the keys to the front door" (Mills 2011, p. 2). One researcher typed some search terms associated with a PLC

(Programmable Logic Controller) in Google, which gave one result that referenced a "RTU pump status… that appeared to be connected to the Internet. The result also included a password – 1234" (Mills 2011, p. 2).

The twelfth case involved Red Tiger Security, a SCADA security consulting firm, also demonstrated how anyone could discover the Internet Protocol address of a PLC when it was connected to the internet, and send it commands that would be executed (Mills 2011). The firm discovered (online) an ABB Transformer running an electricity substation in the United Kingdom that did not require any password for access: "you could see [circuit] breaker statuses, see the last time it was worked on, the status of the transformer… it's still on the internet, but now they prompt for a password" (Mills 2011, p. 3). All the experts agreed that this information and ICS equipment should not have been on the internet.

The above literature identified several notions of ICS threats, vulnerabilities, and consequences (TVCs). Furthermore, it revealed an assortment of factors that could influence offender decision-making processes. However, these TVC concepts and offender decision-making factors were too broad, disorganized, and found in isolation; therefore TVC concepts for this research were defined, offender decision-making factors were categorized into the acronym PARE RISKS, and each of these factors were mapped to TVCs to illustrate their connections.

Threat, Vulnerability, and Consequence Definitions

For the purposes of this research, threat is defined as the intention and capability of an adversary to undertake actions with the potential to cause the loss of, or damage to, an ICS and dependent infrastructure. This framework component has three elements: criminal organization/type – attackers/leisure cybercriminals, bot-network operator, industrial spies, foreign intelligence services, terrorists, professional cybercriminals, criminal groups, phishers, spammers, and spyware/malware authors; motivation – curiosity, spying, thrill/challenge, status, revenge, and monetary gain; and technical expertise – script kiddy, cyberpunks, hackers, crackers, cyber gangs, and information merchants. This expertise is also related to the type of attack strategy used: brute force attack, social engineering, IP spoofing, DDoS, and toolkit, to name a few. The threat-related components are *1. Attack and alliance* properties; and *2. Knowledge, research, and development*. These components directly tie into the 'capable offender' element of Routine Activity Theory (RAT) and also impact the offender's cost-benefit analysis (Rational Choice Theory/RCT).

Vulnerability is a weakness that can be exploited to gain access to a given ICS and subsequent destruction or theft of the ICS and dependent infrastructure. The three types of vulnerabilities identified by NIST Guide to ICS are used for this research: Policy and Procedure, Platform, and Network categories, and as noted earlier, no vulnerability is more prevalent with regards to the likelihood of occurrence or severity of impact if exploited. To summarize the vulnerabilities from the literature review, these include (poor) 3. *Prevention measures*; (the lack of) *4. Security testing, assessments, and audits*; *5. System weaknesses*; and *6. Ease of access* to the system. These components tie into

RAT's 'suitable target' and 'absence of a capable guardian' elements and also impact the offender decision-making process identified by RCT.

Consequence is defined as the effect of an event, incident, or occurrence (DHS Risk Lexicon 2010). Consequences can be categorized in several ways including economic, environmental, health and safety, and operational (DHS Risk Lexicon 2010, Moteff 2005). There is another way of categorizing consequence: direct impact, indirect impact, and industry response. Direct consequences are related to the immediate impact on the electricity infrastructure and include the corruption of information, inaccurate information processing, system modification, denial/disruption of service, and theft of service. Indirect consequences are cascading effects and are of two types. First are the cascading effects within the facility that may result in physical plant equipment damage, environmental damage, safety and health impairment, financial loss, and operational damage. The second cascading effects are those on other (interdependent) infrastructures, such as transportation, communication services, finance and banking, healthcare services, and emergency services. Another consequence of an ICS attack is the response (countermeasure) it generates from the industry. Of course, different consequences have different levels of criticality; the more the loss of an asset "threatens the survival or viability of its owners, of those located nearby, or of others who depend on it … the more critical it becomes" (Moteff 2005). Typically, the degree of criticality is assessed qualitatively as high, medium, or low, or some variation of this measure. Thus, consequences include *7. Results*; *8. Response and recovery*; and *9. Interconnectedness and interdependencies*. Attack consequences can be seen as a reward of offending, which (according to RCT) impacts an offender's cost-benefit analysis. This component is used

by the industry to predict ICS cyberattack risk. Risk (R) is a function of the likelihood (probability) that a defined threat agent (T) can exploit a specific vulnerability (V) and create a consequence (C). It is important to note that the risk is a potential risk; it is a possibility. This relationship can be represented via the equation:

$$R \approx f(T,V,C).$$

This suggests that consequence is also a necessary component for crime, and is therefore included in this research. As noted earlier, this study is exploratory in nature and seeks to identify factors affecting offender cost-benefit analysis; it cannot contribute to quantifying TVCs and therefore cannot offer any formula for risk prediction.

PARE RISKS Framework

The above threat, vulnerability, and consequence definitions are used to sift through the literature to identify specific factors that influence offender decision-making in ICS cyberattacks. Nine factors emerge and are accounted for by the acronym PARE RISKS. Each of the acronym letters corresponds to either a threat, vulnerability, or a consequence (TVC), as is shown in Table 1, following the discussion below.

1. **P**revention Measures: ICS are infamous for poor security measures. This vulnerability dimension measures security practices, such as the use of firewalls, intrusion detection systems, and software patches.
2. **A**ttacks & Alliances: The technical difficulty of the attack, the choice of attack, and the threat agent coincide to determine the characteristics of the cyberattack against ICS. Furthermore, cybercriminals can work alone, in small partnerships, or larger

networks. This threat dimension measures the sophistication, source, choice, and motivation of the attack.

3. **R**esults: Damaging or disrupting ICS can have serious consequences, as noted above. This consequence dimension measures both direct consequence and cascading effects within the electricity sector.
4. **E**ase of Access: Given that ICS are increasingly connected to the internet and are remotely accessible, this vulnerability dimension measures access to the internet, connection speed, remote access, and frequency of remote connectivity.
5. **R**esponse & Recovery: This consequence dimension measures responses to ICS attacks and how these are reported. If a system fails, how long will it take to repair or replace it? This time factor includes time delays inherent in failure diagnosis; repair parts requisition, and fix implementation. This dimension also captures which response agents are perceived as most likely to respond.
6. **I**nterconnectedness & Interdependencies: Understanding system interdependencies enables an evaluation of cascading failures wherein failure of the electricity sector can have damaging effects on one or more additional systems. This consequence dimension measures possible interdependencies between the electricity sector and water, transportation, communication, financial, healthcare, postal sectors, emergency services, and law enforcement.
7. **S**ecurity Testing, Assessments & Audits: Regularly testing and assessing ICS vulnerabilities have strongly been recommended, and in some instances, been implemented. This vulnerability dimension examines whether assessment plans are in place and how regularly these are performed. Conducting security testing and audits

allows for ongoing evaluation of the plant's cyber security defense and early identification of security weaknesses.

8. **K**nowledge, Skills, Research & Development: Cybercriminals may learn skills from, and share information with, each other. Given that information on ICS is easily and publicly available, cybercriminals may spend time researching and developing the most efficient attack. This threat dimension assesses how cybercriminals may share information, learn skills, research targets, and develop attacks accordingly.
9. **S**ystem Weaknesses: Several ICS vulnerabilities have been discussed, and these can be exploited by cybercriminals. This vulnerability dimension assesses system vulnerabilities that can occur due to flaws, misconfigurations, or poor maintenance of their platforms and networks.

Table 1. Mapping PARE RISKS to TVC

	Description	**Threat/Vulnerability/Consequence**
P	Prevention Measures	Vulnerability
A	Attacks & Alliances	Threat
R	Results	Consequence
E	Ease of Access	Vulnerability
R	Response & Recovery	Consequence
I	Interconnectedness & Interdependencies	Consequence
S	Security Testing, Assessments & Audits	Vulnerability
K	Knowledge, Skills, Research & Development	Threat
S	System Weaknesses	Vulnerability

Conclusion

This chapter offered a focused literature review on cyberspace, ICTs, vulnerabilities, threats, consequences (TVCs), and electricity sector cybercrimes. It then defined TVCs for this research and extracted corresponding factors influencing offender decision-making from the literature. Nine decision-making factors emerged and were organized to create the PARE RISKS framework: Prevention measures; Attacks and Alliances; Result; Ease of Access; Response and Recovery; Interconnectedness and Interdependencies; Security Testing, Assessments, and Audits; Knowledge, Skills, Research and Development; and System Weaknesses.

This framework gives rise to two main questions: Do hackers and industry perceive these offender decision-making factors in the same way? Is the PARE RISKS framework correctly modeled to capture cybercriminal offender decision-making in ICS cyberattacks? To answer these questions, test the five research hypotheses, and address the ten research questions identified in Chapter I, hackers and industry are surveyed and interviewed. The next chapter details these methods, focusing on the design and implementation procedures.

Chapter IV. Research Design

This chapter identifies the methods used for this study. The first, brief, section notes the Rutgers University Internal Review Board's approval for this research. The second section explains the use of method triangulation and its relevance to this study. The third section discusses the use of, and justification for, surveys, the units of analysis, sampling strategy, sample size, operationalization strategy, and survey design and implementation. Finally, the use of interviews, and their relevance to this study are discussed. This section also details the units of analysis and sampling strategy, and interview design, implementation, and transcription procedures.

Internal Review Board

This research involved human participants, and as such it was subjected to a review by the Rutgers University Internal Review Board. This study was approved as on June 25, 2010. Because this study was anonymous in nature and only asked participants about their perceptions, it qualified for an exempt review. All survey and interview participants were given an information sheet that outlined the study background and purpose, and also offered contact information for the researcher, supervisor, and the University's review board.

Method Triangulation

Triangulation relates to the use of multiple methods of data collection to study a particular phenomenon (King & Horrocks 2010; Denzin 1978a). Methodological triangulation can be used to obtain a more complete, "holistic, and contextual portrayal of

the unit(s) under study" (Jick 1979, p. 603). The use of different methods may uncover some unique findings that may otherwise have been undiscovered by single methods (Jick 1979). Methodological triangulation is thus relevant in learning about electricity ICS cyberatttacks; it enhances our understanding by allowing for new or deeper dimensions to emerge (Jick 1979).

Data is collected using both surveys and interviews. This mixed methods approach is used for two reasons. First, surveys help identify *where* perception gaps exist, while the interviews shed light on *why* these gaps exist. Understanding both the differences and the reasons for their existence are important in understanding both the technical and administrative elements of prevention measures and practices. Second, while the surveys help identify factors that influence offender decision-making in ICS cyberattacks, the interviews may reveal other factors or more depth on those captured via the surveys.

Surveys

The survey is a non-experimental, descriptive research method, which uses a standard set of questions administered in a uniform manner. This research employs a cross-sectional survey, which is used to collect information on a population at a single point in time. The first goal of this research is to understand hacker and industry gaps in their perceptions of Threats, Vulnerabilities, and Consequences (TVCs). One way to discover how TVCs are perceived is through the use of surveys, which asks multiple respondents about their beliefs, opinions, characteristics, and past or present behavior (Neuman 2003; Maxfield & Babbie 2005; Yin 2008). Surveys are useful to collect data

on phenomena that cannot be directly observed (Neuman 2003). The offender decision-making process during ICS cyberattacks cannot be observed as they are clandestine and go undetected. As such, surveys offer a means to identify the factors that may influence offender decision-making processes, making it an appropriate choice to fulfill the second goal of this study.

Units of Analysis, Sampling Strategies, and Sample Size

The units of analysis for the proposed research were individuals from two domains: electricity and hacking communities. While obtaining a random, representative sample would have been ideal for this study, it was impossible given the covert, dynamic, and illicit nature of ICS cyberattacks. As such, a non-probability convenience sampling strategy was employed for this exploratory study, which involved selecting units of analysis on the basis of project relevance (Maxfield & Babbie 2005). This sampling technique was appropriate given the exploratory nature of this research and for selecting individuals from a "difficult-to-reach, specialized population", such as cybercriminals (Neuman 2003, p. 213; Maxfield & Babbie 2005). The purposive sampling technique was then followed by snowball sampling, which permitted access to individuals that were not identified previously.

Survey data for the industry was collected from four sources. The survey was advertised and promoted through the North American Electric Reliability Corporation (NERC), the System Administration, Networking, and Security (SANS) infrastructure conference, and EnergySec and SCADASEC mailing lists. NERC's primary responsibility was to ensure the reliability of the power system in North America. NERC

accomplished this via developing and enforcing reliability standards, monitoring the bulk power system, and educating, training, and certifying industry personnel (NERC 2010). Additionally, NERC coordinated electric industry activities that were designed to protect the industry's critical infrastructure from cyber threats, which made it an ideal organization to accost. While the identities and roles of the NERC respondents remained unknown, they were either responsible for managing security operations or plant operations.

The SANS Institute was one of the largest sources for information security training and security certification in the world. It also developed, maintained, and made available the largest collection of research documents about various aspects of information security training (SANS 2011b). The SANS Institute held a SCADA North American 2011 Summit in February 2011 in Florida. Conference attendees were ICS and SCADA experts and thus offered a representative set to sample from. Two critical infrastructure mailing lists were also used to advertise the survey. The Energy Sector Security Consortium (EnergySec) was a private forum of information security, physical security, audit, disaster recovery, and business continuity professionals from energy industry asset owners (EnergySec 2011). As such its mailing list provided a diverse member base in the energy sector. Finally, the SCADASEC mailing list was also used to advertise the survey. SCADASEC provided a common forum to discuss security concepts regarding publicly known vulnerabilities and exploits that affected ICS (infracritical.com 2011). The mailing list included government personnel, IT security professionals, SCADA security professionals, and homeland security professionals, to name a few,

which also served as a relevant pool to draw from (infracritical.com 2011). A total of 121 industry responses were obtained via these four avenues.

Information attained from cybercriminals would have been useful in understanding target selection, attack technique, attack patterns, and offender decision-making in general (Decker 2005). However, accessing this population, especially in the realm of cybercrimes against critical infrastructures, was problematic because they belonged to an underground culture that was unknown or inaccessible. Apprehended cybercriminals would also have been useful in understanding decision-making factors, and in particular bounded rationality. Identifying the individuals who targeted the electricity sector, however, was also problematic. First, most of the electricity sector cyberattacks were not publicized. Second, the few cyberattacks that were publicly disclosed were often through the media and not official government, security, or industry sources, which raised issues of credibility. Third, when the sources of attacks were disclosed, they were often foreign-based or nation-sponsored, and hence raised several issues, such as identifying the specific source(s) or individual(s), jurisdictional access, and ethical approval spanning geographic borders. Collectively, these issues were beyond the scope of the current exploratory study.

Thus, ethical hackers offered a logical alternative as they possessed the technological savvy to conduct cybercrimes but without the malicious intent of cybercriminals. Survey data for the hacking community was obtained entirely from the three-day 2010 DEFCON hacking conference in Las Vegas. DEFCON was one of oldest and largest hacker conventions, with approximately 5,000 to 7,000 attendees. Conference attendees had knowledge about hacking techniques, and general attack trends, making

them an appropriate participant pool to draw from. A total of 202 respondents were sampled from DEFCON. Both domains were also asked to refer other members of their respective communities, who were then directed to the survey.

Survey Design, Operationalization, and Implementation

The survey was comprised of closed-ended questions, which gave the participants fixed responses to choose from [Appendix A]. Closed-ended surveys were easier and quicker for respondents to answer. Furthermore, multiple responses from closed-ended questions were easier to compare. The language and wording for this survey was based on the 2008 National Institute of Standards and Technology (NIST) guide for Industrial Control Systems (ICS). This guide offered a detailed list of the assortment of ICS vulnerabilities and threat agents. While this guide provided the foundation necessary to assist with the survey planning, the research survey designed in this study took the NIST guide a step further by (i) categorizing the various vulnerabilities along the PARE RISKS model, (ii) adding the human factor of cybercrimes by accounting for motivations, alliances, research and development, and resources (skills, money, and time), and (iii) comparing the difference in perceptions of hackers and industry experts.

Hackers and industry were given a preliminary survey to test its clarity and completeness, and assess the language, quality, and breadth of the survey questions. This initial screening revealed a few unanticipated problems with question wording, survey length, and survey completion time. The corresponding feedback was utilized to refine the survey. A pilot study was then conducted with one DEFCON chapter to identify any further issues with regards to question clarity, survey design and length, and survey

completion both in online and paper formats. This study yielded minor feedback and revisions, which were then used to further refine the survey.

As identified earlier, PARE RISKS identified factors that make ICS systems susceptible to cyberattacks. The survey therefore was divided into nine sections, each containing questions to measure the nine factors influencing offender decision-making. Questions were as specific as possible so as to accurately measure each vulnerability dimension (Maxfield & Babbie 2005). For instance, survey items from *different* PARE RISKS factors were not be framed in one question: "Are vulnerability assessments and security patches regularly conducted?". A 'yes' response would not indicate which dimension (assessment or security) the respondent was agreeing to. Similarly, a 'no' response gave no indication of which dimension the respondent did not perceive as regularly being conducted. Furthermore, survey items from the *same* factor were also not put into one question: "Are firewalls and anti-virus updates regularly conducted?" A 'yes' response would indicate that respondents perceived firewall updates, or anti-virus updates, or both, were regularly updated. A 'no' response indicated that respondents perceived that neither or one was not being updated, resulting in data that could not be disaggregated. Each question therefore accounted for one item relating to a single factor. The PARE RISKS model was operationalized as noted below. The Interconnectedness and interdependencies factor was grouped with the Result factor as they both were consequences of ICS cyberattacks; the former being an indirect consequence, while the latter was direct:

1. Prevention Measures: This dimension was measured with six questions, which asked about firewall and antivirus updates, bypassing intrusion detection systems, and the

amount of time spent countering security measures. All responses were rank-order items. For instance, the ease of bypassing intrusion detection systems was measured on a scale of 1-5, where 1 was easy and 5 was difficult. Higher scores, therefore, reported stronger prevention strategies.

2. *Attacks & Alliances:* This dimension was measured with five questions, which asked about cybercriminal profiles, attack motivation, attack technique, the likelihood of working individually or in alliances, and how alliance members found each other. All responses were rank-order items. For instance, terrorists as a possible attack source was measured and given a rank between 1 and 5. Higher scores, therefore, suggested that terrorists were perceived as a more likely offender.

3. *Result, Interconnectedness, and Interdependencies:* This dimension was measured with three questions, which asked about attack consequences on electricity services and electricity-dependent infrastructures. All responses were rank-order items. For instance, the corruption of information as a possible consequence on the electricity sector was measured and given a rank between 1 and 5. Higher scores, therefore, reported a more likely consequence.

4. *Ease of Access:* This dimension was measured with six questions, which asked respondents about attack frequency, remote access to ICS, email and internet exploits, and connection speed. Response categories included binary agree/disagree statements, which were coded as 1/0 respectively. Rank-order items were also included. For instance, the usefulness of a wide area network (WAN) to cybercriminals in conducting their attacks was ranked on a scale of 1-5, where 1 was the least ideal and 5 was the most

ideal. Higher scores, therefore, reported that a WAN was very useful for cybercriminals to conduct attacks.

5. *Response and Recovery:* This dimension was measured with six questions, which asked about response agencies, response rates, counter-attack rates, and evasion strategies. All responses categories included rank-order items. For instance, how likely the Federal Bureau of Investigation (FBI) would be expected to respond to a cyberattack was ranked on a scale of 1-5, where 1 was the least likely to respond and 5 was the most likely. Higher scores, therefore, indicated that the FBI was perceived as more likely to respond to a cyberattack.

6. *Security Testing, Assessment, and Audit:* This dimension was measured with eight questions, which asked respondents about security policies, administrative policies, testing frequencies, and vulnerability assessments. Response categories included binary agree/disagree statements, which were coded as 1/0 respectively. Rank-order items were also included. For instance, security testing frequency was measured as Daily; weekly; monthly; quarterly; semi-annually; annually; less than once a year, and was given a rank between 7 and 1 respectively. Higher scores, therefore, represented more frequent security testing. In order to maintain the similar 1-5 scale as other PARE RISKS factors, the coding was transformed via SPSS as follows: scores of 1 remained the same; scores of 2 and 3 were recoded to a score of 2; scores of 4 were recoded to a score of 3; scores of 5 and 6 were recoded to a score of 4; and scores of 7 were recoded to a score of 5.

7. *Knowledge, Skills, Research & Development:* This dimension was measured with six questions, which asked respondents about hacking forums, knowledge sharing, and skill sets. Response categories included binary agree/disagree statements, which were

coded as 1/0 respectively. Rank-order items were also included. For instance, the threat-level of allied cybercriminals based on past successful partnerships was ranked on a scale of 1-5, where 1 was less threatening and 5 was the most. Higher scores, therefore, indicated that alliances created based on past successful partnerships were perceived as a greater threat to ICS.

8. *System Weaknesses:* This dimension was measured with four questions, which asked about hardware and software vulnerabilities, communication vulnerabilities, and configuration vulnerabilities. Response categories included binary agree/disagree statements, which were coded as 1/0 respectively. Rank-order items were also included. For instance, unsecured physical ports as an exploitable vulnerability were measured and scored as 1,2,3,4, and 5. Higher scores, therefore, indicated that unsecured physical ports were perceived as a highly exploitable vulnerability.

The layout of the questionnaire was also important. First, the questionnaire did not use too many colors or fonts as these distracted participants; bolding section headings for each factor and the key elements within each factor made the questions easier to read and understand (Maxfield & Babbie 2005; surveysystem.com 2009). Second, the questionnaire only employed minimum text for each question and the appropriate form element (multiple choice, rating scale, and open ended text) for the answer; graphics and images were not employed as these were unnecessary and also distracted participants (Tourangeau 2004).

The survey was offered in two formats: paper-based and online. Paper-based surveys were administered at the DEFCON and SANS conferences, which permitted the researcher to address any respondent questions and concerns on site. The online survey

was hosted via Surveymonkey.com. Surveymonkey was an online survey site that simplified the survey process considerably. Surveymonkey offered 17 formats for asking questions (multiple choice, true false, open-ended, etc), which provided flexibility in survey design and data collection. The site allowed data to be exported, which could then be analyzed via programs like SPSS. Finally, anonymity was attained using Surveymonkey's software by changing the 'save IP address' setting, so that respondent locations and computer information were not stored. Furthermore, Surveymonkey offered Secure Sockets Layer (SSL) encryption, which was used to transfer private documents and permitted downloading collected data over a secure channel. All hacker responses were paper-based. Only twelve industry responses were completed online, while the paper-based surveys accounted for the remaining 109 industry responses. Finally, the research study and survey were advertised via each of the hacker and industry avenues of data collection to increase the response rate. When the surveys were conducted at DefCon and SANS, a few participants recommended individuals with ICS expertise, who were then approached to participate in phone interviews.

Interviews

The survey was used to identify gaps in hacker and industry perceptions. However, the survey had close-ended questions, which did not give respondents the opportunity to address why these gaps may have existed. Semi-structured interviews made up for this shortcoming; they allowed for the exploration of *why* respondent perceptions differed (Carr & Worth 2001). To achieve depth and roundness of understanding TVCs, accessing participants' contextual accounts and experiences was

crucial (Mason 2002). As noted earlier, the survey was primarily designed using the NIST guide, which was purely technical. The survey therefore included minimal questions identifying the human component of cybercrimes, such as alliances, motivations, and skills in the context of ICS cyberattacks. This information, however, was based on the literature review and only offered a rudimentary set of factors. Thus, a second, equally important, justification for using interviews was to identify any factors that had not been listed in the survey, which contributed to the offender decision-making processes

Units of Analysis, Sampling Strategies, and Sample Size

The units of analysis were the same as for the surveys, namely individuals from the electricity sector and the hacking community. Non-probability sampling was used here as well. A few survey participants from both hacking and industry domains recommended other contacts who would be willing to participate in the interviews. As ICS expertise was limited in the industry and hacking communities, these initial subjects were crucial in gaining access to other participants.

King and Horrocks (2010) noted that there were three means of gaining access to this expert population. First, potential participants must be reached through a gatekeeper, who had the authority to grant permission to, or facilitate, access potential participants (King & Horrocks 2010). For instance, DefCon, NERC, SANS, and EnergySec all served as gatekeepers; these organizations provided access to potential participants, a few of which were successfully recruited for the interview. Special permission was received from DefCon and SANS to attend their conferences and a one page IRB-approved

advertisement was used to recruit interview participants. Second, King and Horrocks (2010) noted that researchers also used one or more insiders to actively assist in recruiting participants, who may identify qualified participants, and pass project information sheets requesting participation to them. Indeed, some participants working in ICS security and approached their own contacts and electricity sector clients to participate in the interview. Snowball sampling was a third way of gaining access to subjects, where researchers used the initial few interviewees to recommend other potential participants who fit the inclusion criteria for the study (King & Horrocks 2010). A few of the interview subjects for this study recommended other, potential subjects, who were then approached for participation. All three approaches resulted in a total of seven interview subjects; three hackers and four industry experts were interviewed.

Interview Design, Implementation, and Transcription

The interview guide had three sets of questions [Appendices B and C]. *Background* questions were used at the introduction, which were straightforward descriptive questions about the personal characteristics of subjects, such as their occupation and their work trajectory (King and Horrocks 2010). *Knowledge* questions were used to set the context for the interview. This category related to questions about factual information the participant held. These questions asked participants how they defined threats, vulnerabilities, consequences, and risks, and were based on the corresponding literature review themes identified in Chapter III. The third type of questions used formed the majority of the interview guide. The *opinion* questions asked participants about the topic at hand (King and Horrocks 2010). These included questions

such as ‘How would hackers and industry think differently about (electricity) ICS threats, vulnerabilities, and risks?’. Knowledge questions differed from opinion questions in that the former considered what the participant believed to be a fact and not with whether it was actually true in any objective sense (King and Horrocks 2010).

The interview guide complemented and supplemented the surveys by permitting interviewees to (i) expand on their notions of threats, vulnerabilities, and consequences, (ii) offer examples based on their experiences, (iii) discuss case studies in a detailed manner, and (iv) delve into offender decision-making and cost-benefit analysis. The PARE RISKS model was operationalized at the higher level of TVCs as this gave the interviewee more freedom to be creative rather than being guided by preset factors. These open ended questions gave them much more flexibility than the yes/no response to the corresponding survey question. Additionally, several probes and prompts were formulated for the interview to obtain the most detailed account possible from interview subjects. Probes were follow-up questions that encouraged participants to expand on initial answers to obtain more depth in their responses (King & Horrocks 2010). Prompts were interventions that clarified the meaning of a question for interviewees, when they expressed uncertainty about that question (King & Horrocks 2010). A draft copy of the interview guide was sent to both hackers and industry for their feedback, which was then used to refine the guide

Telephone interviewing was used to collect data. As defined by Carr and Worth (2001), a telephone interview in “research terms [was] a strategy for obtaining data which allow[ed] interpersonal communication without a face-to-face meeting” (p. 512). This method facilitated the inclusion of participants who were geographically dispersed and

distant from the interviewer, without requiring time-consuming and expensive travel or recruitment and training of local interviewers (Carr & Worth 2001; King & Horrocks 2010). Furthermore, phone interviewing had been viewed as a legitimate data collection method for research, with phone interviews producing data which were comparable in quality to that received via face-to-face interviews (Carr & Worth 2001; King & Horrcks 2010). Some of the advantages to using this method included smaller interviewer effects or lower tendency to socially desirable responses (Carr & Worth 2001; King & Horrocks 2010).

The interviews were approximately one hour and thirty minutes in duration and, like the surveys, were anonymous. Each interviewee was read the informed consent form and given the contact details for the candidate, supervisor, and the IRB. When the subjects agreed to participate, the interview process formally began. Telephone interviews were recorded using a digital recorder, which stored all the files in an mp3 format that could easily be downloaded to, and played on, the computer. Recording the conversation enabled the interviewer to respond directly to the subject as her attention was not consumed by writing notes (Carr & Worth 2001). However, notes were also taken to accompany the audio recording as they served as probes, which could be pursued later rather than interrupting subjects in mid-flow (King & Horrocks 2010).

Interviews were transcribed at the basic level – only the actual words spoken were recorded. In a few instances, the subjects' responses were unclear or inaudible. These words or phrases were marked accordingly, rather than inserting a best guess (King & Horrocks 2010). Transcriptions were saved as a MS Word document and randomly numbered with either 'hacker' or 'industry' suffixes to filenames to maintain the

anonymity of participants. After the response to each question was transcribed, a timestamp was included to cross-reference the transcribed text to the original audio interview file.

Conclusion

This chapter made the case that surveys and interviews provided an appropriate means for gaining a plausible first picture of cybercrimes against electricity sectors. Surveys and interviews were chosen because their ability for 'discovering' phenomena fit nicely with the exploratory nature of this research. While the surveys were justified as being useful in identifying where perception gaps existed, the use of interviews was relevant in offering insight into why these gaps existed. Furthermore, the interviews supplemented surveys by identifying any offender decision-making factors that did not emerge in the surveys. Each step in this methodology reflected the research objectives and hypotheses, which ensured that the data remained true to the research interests. What did the data reveal about hacker and industry perceptions of threats, vulnerabilities, and consequences? What caused the difference, if any, in their perceptions? What factors influenced offender decision-making? The next chapter identifies the data analysis procedures and the strengths and limitations of this study.

Chapter V. Data Analysis, Results & Findings

This chapter presents the analytical strategy, results and findings of this study. First hackers and industry perception gaps with regards to threats, vulnerabilities, and consequences (TVCs) are discussed. Additionally, a thematic analysis of interview data reveals why these gaps occur. The second section identifies the factors that influence offender decision-making. Here, an exploratory factor analysis is conducted to identify any underlying latent variables. Interview data is subjected to a second thematic analysis to also identify any additional decision-making factors. The third section discusses the adequacy of the PARE RISKS framework. The next section addresses the strengths and limitations of the data. Finally, this chapter offers a discussion on the interpretation of the results and compares this perception-based study with actual ICS cybervulnerability assessments.

Perception Gaps: Analysis & Results

The first goal of this study is to identify hacker and industry perception gaps, if any, on ICS TVCs, and why these gaps exist. This goal corresponds to the first three research hypotheses. As the survey items are ordinal and categorical, non-parametric tests are used as the assumption cannot be made that the underlying population fits a normal (or any other parameterized) distribution (Bertram 2007). Mann-U and chi-square tests are used in SPSS to compare hacker and industry opinions. While the surveys offer insight on which factors are perceived differently by hackers and industry, the interviews shed light on *why* participants believe these gaps exist. NVivo 9 is used to code the

interview transcripts. NVivo 9 is a software that classifies, sorts, and arranges information, by creating nodes (themes) and sub-nodes (sub-themes) as they emerge (QSR International 2011a, 2011b). There is no theoretical guidance to identify initial themes and as such the data is scanned to identify common themes that emerge in the interview transcripts. Four main themes emerge in the data offering insight into why hacker and industry perceptions differ: consensus on TVC definitions; different goals; different knowledge bases; and inadequate, poor or incorrect communication.

The survey results are presented first to identify where gaps exist, which are followed by interview results that reveal why these gaps exist. It is important to note that these results are based on hacker and industry *perceptions* and not on any direct data. The significant results listed below are therefore based on indirect perceptual data, which should be interpreted tentatively.

Hypothesis 1: Hackers and industry experts differ in their perceptions of threats

Using Table 1. (p.31), two of the PARE RISKS factors are used to test this hypothesis: Attacks & Alliances and Knowledge, Skills, Research & Development, as they map to the 'threat' component of TVC. The significant results for these factors are:

1. Attacks & Alliances:
    a. Industry representatives (Mdn 4.0) perceive that malware is the most likely used technique in attacking ICS significantly more than hackers (Mdn 3.0), $U=6152.0$, $p<.05$ $r=-.16$.
2. Knowledge, Skills, Research & Development
    a. There is a significant association between the type of respondent and whether or not he/she perceives that cybercriminals access ICS hacking forums $\chi^2(1,$

N=285) = 8.897, p<.05. Hackers are significantly more likely than industry to believe that cybercriminals access ICS hacking forums.

Hypothesis 2: Hackers and industry experts differ in their perceptions of consequences.

Three of the PARE RISKS factors are used to test this hypothesis: Results; Response & Recovery; and Interconnectedness and Interdependencies as they map to the 'consequence' component of TVC. The significant results for these factors are:

1. Results:
    a. Industry representatives (Mdn 4.0) perceive that the greatest impact on electricity services should an ICS attack occur is information corruption significantly more than hackers (Mdn 3.0), U=6549.5, p<.05 r=-.18.
    b. Industry representatives (Mdn 3.0) perceive that the greatest impact on electricity services should an ICS attack occur is inaccurate information processing significantly more than hackers (Mdn 3.0), U=7047, p<.05 r=-.12.
    c. Industry representatives (Mdn 4.0) perceive that the greatest impact on electricity services should an ICS attack occur is denial/disruption of service significantly more than hackers (Mdn 5.0), U=7047, p<.05 r=-.2.
    d. Industry representatives (Mdn 5.0) perceive that the most devastating impact should an electricity ICS attack occur is physical in nature (damage to plant equipment) significantly more than hackers (Mdn 4.0), U=6676.5, p<.05 r=-.2.

2. Response & Recovery:

    a. Industry representatives (Mdn 4.0) perceive that cybercriminals are most worried about CERT if they are detected significantly less than hackers (Mdn 4.0), U=6867.5, p<.05, r=-.07.

    b. Industry representatives (Mdn 3.0) perceive that cybercriminals are most worried about (local) police departments responding to an attack if they are detected significantly more than hackers (Mdn 3.0), U=6879.0, p<.05, r=-.12.

Hypothesis 3: Hackers and industry experts differ in their perceptions of system vulnerabilities and prevention measures.

Four of the PARE RISKS factors are used to test this hypothesis: Prevention Measures; Ease of Access; Security Testing, Assessments & Audits; and System Weaknesses, as they map to the 'vulnerability' component of TVC. The significant results for these factors are:

1. Prevention Measures:

    a. Industry representatives (Mdn 2.0) perceive that bypassing Host IDS network detection systems (such as tripwire, fileagent) is harder significantly more than hackers (Mdn 3.0), U=7255, p<.05, r=-.12.

2. Ease of Access:

    a. There is a significant association between the type of respondent and whether or not he/she perceives that internet access is exploited $\chi^2(1) = 4.027$, p<.05. Hackers are significantly more likely than industry to believe that internet access is exploited.

b. There is a significant association between the type of respondent and whether or not he/she perceives that email access is exploited $\chi^2(1) = 6.886$, $p<.05$. Hackers are significantly more likely than industry to believe that email access is exploited.

3. Security Testing, Assessments & Audits:

   a. There is a significant association between the type of respondent and whether or not he/she perceives that security testing is effective $\chi^2(1) = 8.354$, $p<.05$. Hackers are significantly more likely than industry to believe that security testing is effective.

4. System Weaknesses:

   a. Industry representatives (Mdn 4.0) perceive that passwords not encrypted in transit is an ideal vulnerability to exploit for an ICS attack significantly less than hackers (Mdn 5.0), $U=7246.5$, $p<.05$, $r=-.16$.

The above significant differences demonstrate that there are important differences in how hackers and industry perceive ICS TVCs. The interview analysis reveals why these gaps exist. Hackers and industry both agreed that there are oftentimes confusion as to what the terms threat, vulnerability, and consequence meant to both domains. As one hacker notes:

> "… people **do not understand** what risk is. **They will confuse threat, vulnerability, and risk** and not actually understand what it is … but the problem is that the reason we don't understand how to really define risk is because **there is no consensus on how we define threat, vulnerability, and consequence**, which is funny as hell…" – *Hacker 2*

Hackers and industry perceptions also vary because of their respective roles, and hence their corresponding goals. Both hackers and industry are concerned with different priorities and have minimally overlapping responsibilities:

> "I think management is focused on business for sure. They have a **business goal and objective**… You move down the line to pen tester, they're there trying to circumvent the security that's in place… **they're just there to see what they can break into** …" – *Hacker 1*

> "I like to [take my customers' **downtime numbers] because that's something that operations managers, directors, and vice presidents typically understand**… So if you put it in those terms, security becomes quote unquote easier to sell." – *Industry 1*

A third reason for perception differences is the different knowledge possessed by both hackers and industry, which is an extension of their respective roles. Hackers and industry agree that non-technical members of the electricity sector do not comprehend the importance of security, vulnerability, and prevention measures:

> "And it took **quite a lot to help educate those guys on what risks are**. I mean, the initial discussion with those guys was 'hey – this is regulatory stuff called FERC and NERC, and you know – what do we need to worry about' – I'm like 'oh good grief – oh god' – Ok people – let's do little bit of education first." – *Hacker 3*

> "The SCADA industry professionals have **relatively limited technical expertise** at implementing security controls. Their employers have not put a lot of effort into changing that situation." – *Industry 4*

Finally, hackers feel that there is poor communication between themselves and industry, and when communication does occur, it seldom results in any positive or effective action that improves ICS security:

> "I think this is where there is some lacking steps and **miscommunication** in what people are trying to do to secure the cyberworld." – *Hacker 1*

> "But again, I'll be perfectly honest. There's stuff out there that we've released deliberately straight out into the public because the **companies haven't listened**." – *Hacker 3*

Offender Decision-Making Factors: Analysis & Results

The second goal of this study is to identify the factors that influenced offender decision-making in ICS cyberattacks. This goal corresponds to the last two research hypotheses. Exploratory factor analysis (EFA) is conducted to discover the factor structure of a measure and to examine its internal reliability. This section details the analytic strategy used to conduct EFA, focusing on factor extraction method, retention criterion, and rotation technique. The factors retained from EFA are supplemented with the factors retained from interview analysis. This section also explains the coding and analytic strategy for interview data. Collectively, these two analytic strategies yield a plausible set of factors that influence offender decision-making.

Exploratory Factor Analysis

As discussed in the 'Literature Review & PARE RISKS Framework' chapter, the survey measures suitable targets using the 'entry point for access' and 'system weaknesses' factors of the PARE RISKS model. The absence of a capable guardian is measured using the 'prevention measures' factor. Finally, the potential offender is measured via the 'attacks and alliances' and 'knowledge, skills, research, and development' factors. However, as this research is exploratory in nature, and the researcher has no strong a priori theories about the number and nature of the underlying factors, an exploratory factor analysis (EFA) is conducted (Grant & Fabrigar 2007; Costello & Osborne 2005; Newsom 2005). EFA is typically used to discover the factor

structure of a measure and to examine its internal reliability (Newsom 2005). The goal of EFA is to help determine whether measured variables can be explained by underlying factors (latent variables) that cannot be directly measured, but influence the measured variables (Grant & Fabrigar 2007, p. 332; Costello & Osborne 2005).

Research suggests that when conducting an EFA, there should be approximately 10 cases per survey item (Field 2005; Costello & Osborne 2005). This is not possible with the data set for this research. The survey has 122 items, which would require a dataset of 1,220 cases. However there are only 322 cases. To ensure that the subject to item ratio is at least 10:1, the PARE RISKS factors are logically grouped into hypothetical categories: SPAARR, as noted below in Table 2:

Table 2: Regrouping of PARE RISKS to SPAARR

SPAARR	PARE RISKS	Items	Subject: Item Ratio
System	**E**ase of Access + **S**ystem Weaknesses	38	11:1
Preventative	**P**revention Measures + **S**ecurity Testing, Assessments and Audits	10	32:1
Attackers	**A**ttacks & Alliances + **K**nowledge, Skills, Research & Development	23	14:1
Attacks	**A**ttacks & Alliances + **K**nowledge, Skills, Research & Development	18	18:1
Reactive	**R**esponse & Recovery	21	15:1
Result	**R**esults + **I**nterconnectedness & Interdependencies	22	14:1

Factor Extraction Method, Retention Criterion, and Rotation Technique

Fabrigar et al. (1999) state that if the data are relatively normally distributed, maximum likelihood is the best choice because "it allows for the computation of a wide range of indexes of the goodness of fit of the model [and] permits statistical significance testing of factor loadings and correlations among factors and the computation of

confidence intervals" (p.277). Furthermore, Gorsuch (1989) recommends using maximum likelihood if only a few iterations are performed. If the assumption of multivariate normality is "severely violated", which is the case here, Fabrigar et al. (1999) and Costello & Osborne (2005) recommend using one of the principal factor methods, which is the Principal Axis Factoring extraction method in SPSS.

The Kaiser criterion is first used to determine the number of factors to be retained. This criterion retains all factors with eigenvalues greater than 1.0; however as this method is considered to be the least accurate in retaining factors because of its arbitrariness, the Scree test is used (Ferguson & Cox 1993; Costello & Osborne 2005; Grant & Fabrigar 2007). The scree plot is a graph of eigenvalues, plotted from the greatest value to the smallest. This graph is examined to determine where the last major drop in eigenvalues occurs (Grant & Fabrigar 2007). Those factors that precede the last major drop are retained, and this strategy is considered a reasonable factor retention criterion in the literature (Grant & Fabrigar 2007; Costello & Osborne 2005; Newsom 2005).

While rotation cannot improve the basic aspects of the analysis, such as the amount of variance extracted from the items, it does simplify and clarify the data structure (Costello & Osborne 2005). An oblique rotation method is used, which allows the factors to correlate (Costello & Osborne 2005). Specifically, the direct oblimin method with the default delta (0) value is used. Stevens (1992) states that for a sample size larger than 200, factor loadings greater than .364 are considered significant. Tabachnick and Fidell (2007) recommend .33 as a minimum cutoff for a factor loading. For this research, factor loadings that are larger than 0.3 are reported, as this cutoff is

conventionally regarded as a "meaningful loading" (Pedhazur & Schmelkin, 1991, p.603).

While the retained factors account for most of the variance, the remaining factors also account for some variance, and as such a second EFA is conducted forcing all items to load on the retained factors. Cronbach's α indicates the reliability of a scale; reliability simply means that a scale consistently reflects the construct it is measuring. A value between .7 and .8 is an acceptable value for Cronbach's α, although a lenient cut-off of .60 is common in EFA (Field 2005). The above factor extraction method, retention criterion, and rotation technique are used for all the SPARR groupings. The second EFA for the Preventative grouping is discussed in the body of this dissertation; the remaining SPARR second EFAs are documented in Appendix D.

Hypothesis 4: The factors in the pre-attack environment that impact offender decision-making processes include prevention measures, alliances, result, accessibility, security testing, target reconnaissance, and exploitable weaknesses.

As noted earlier, the analysis results are based on hacker and industry *perceptions*; the factors that influence offender decision-making are therefore based on indirect perceptual data, which should be interpreted tentatively. Five of the six SPAARR factors are used to test this hypothesis: System; Preventative; Attackers; Attacks; and Result. The Preventative category includes survey items for the Prevention Measures and Security Testing, Assessments, and Audits. This category has 10 items, and with a pairwise deletion the subject count varies from 197 to 283, which results in subject to item ratio of 19:1 to 28:1 respectively. For the KMO index of sampling adequacy, values

above 0.6 are required for a good factor analysis. The value of 0.594, as indicated in Table 3, is close to this value.

Table 3: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.594
Bartlett's Test of Sphericity	Approx. Chi-Square	454.615
	Df	45
	Sig.	.000

Table 4 below identifies the initial eigenvalues and proportions of variance explained by each factor. The scree plot for the first EFA on the Preventative category suggests that four factors are to be retained. The second EFA is therefore done with four fixed factors, which are extracted in the factor solution. Looking at the proportions of variance, the bulk of the variance attributable to the retained factors is explained by the first (general) factor (24% out of 68%) in the initial solution, whereas the variance is slightly more evenly distributed in the rotated solution (19.82%, 13.87%, 10.33%, 8.4%).

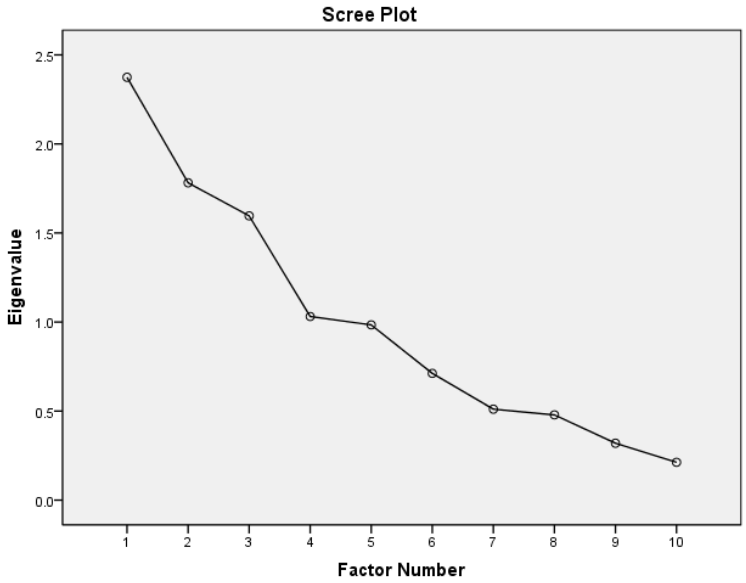
Table 4: Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]	
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance
1	2.374	23.741	23.741	2.046	20.459	20.459	1.982	19.82
2	1.782	17.817	41.559	1.422	14.216	34.675	1.387	13.87
3	1.596	15.961	57.519	1.118	11.181	45.856	1.033	10.33
4	1.031	10.310	67.829	.394	3.944	49.800	.840	8.40
5	.984	9.839	77.668					
6	.712	7.117	84.785					
7	.511	5.108	89.892					
8	.479	4.787	94.679					
9	.319	3.194	97.874					
10	.213	2.126	100.000					

Extraction Method: Principal Axis Factoring.
a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Next, the scree plot (Figure 1) gives an indication of how many factors are to be retained. The change in slope, or the 'elbow', is a useful guide. In the plot below, there is no clear elbow indicating a suitable number of factors to retain. The first, possible elbow suggests a four-factor solution. The second possible elbow suggests a seven-factor sulution, which results in too many (probably irrelevant or meaningless) factors. Therefore, the Kaiser criterion is used instead of the scree plot, and a four-factor solution is considered.

Figure 1: Scree Plot for the Preventative Category



To determine what these factors are, the pattern matrix (Table 5, below) is analyzed. The *first* factor is readily interpretable as protection updates, with high loadings of antivirus software updates (.963), security patch updates (.781), and firewall updates (.639). The *second* factor is readily interpretable as security testing and vulnerability assessment frequency, with high loadings of security testing frequency (.882), and vulnerability assessment frequency (.775). The *third* factor is readily interpretable as

bypassing intrusion detection systems, with loadings of bypassing Host intrusion detection system (.583), bypassing network detection systems (.532), and bypassing other intrusion detection system (.463). The *fourth* factor is also readily interpretable as bypassing intrusion detection systems, with loadings of bypassing perimeter access logging (.650) and bypassing network detection systems (.439). However, as this factor overlaps with the third factor, it is not retained, resulting in a *three-factor solution*.

This solution does not have factor purity, as the bypassing network detection systems item loads on the third and fourth factors, so the factors are not clearly defined by the groupings of tests that load on them. Additionally, these factors do not have five or more strongly loaded items (.50 or better), which would have been desirable and indicative of a solid factor (Costello & Osborne 2005). The identification of these factors, while rudimentary and weak, reflect the exploratory nature of this research, and can be used as a foundation for future studies that should attempt to obtain larger samples (Costello & Osborne 2005).

Table 5: Pattern Matrix[a]

	Factor			
	1	2	3	4
AntivirusSoftwareUpdates_1	.963			
SecurityPatchUpdates_1	.781			
FirewallUpdates_1	.639			
SecurityTestingFrequency_7		.882		
AssessmentFrequency_7		.775		
TimeSpentCounteringSecurity Measures_1				
BypassIDSEaseHostIDS_1			.583	
BypassIDSEaseNetworkDetect ionSystem_1			.532	.439
BypassIDSEase_1			.463	
BypassIDSEasePerimeterAcce ssLogging_1				.650

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 8 iterations.

It is worth knowing whether a scale defined by factor loadings is really measuring a unitary construct. The usual index of the internal consistency of a scale is, as noted above, Cronbach's α. As noted earlier, a value between .7 and .8 is an acceptable value for Cronbach's α, although a lenient cut-off of .60 is common in EFA (Field 2005). For the three items comprising the protection updates factor, the Reliability Statistics (Table 6) indicates an α = .827. The Item-Total Statistic (Table 7) assists in determining whether the removal of one or more items can improve the internal consistency of the remaining items. Cronbach's α improves slightly by removing the 'firewall updates item' (.865).

Table 6: Reliability Statistics

Cronbach's Alpha	N of Items
.827	3

Table 7: Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
FirewallUpdates_1	7.5792	1.575	.587	.865
AntivirusSoftwareUpdates_1	7.3087	1.402	.786	.655
SecurityPatchUpdates_1	7.3989	1.647	.698	.754

For the two items comprising the security testing and vulnerability assessment frequency factor, the Reliability Statistics (Table 8) indicates an α = .808. The Item-Total Statistic (Table 9) indicates that the reliability would not be improved by removal of any of the items.

Table 8: Reliability Statistics

Cronbach's Alpha	N of Items
.808	2

Table 9: Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
SecurityTestingFrequency_7	5.61	2.652	.678	.
AssessmentFrequency_7	5.64	2.730	.678	.

For the three items comprising the ease of bypassing intrusion detection systems factor, the Reliability Statistics (Table 10) indicates an α =.571. The Item-Total Statistic (Table 11) indicates that the reliability would not be improved by removal of any of the items. The α reliability is extremely low, which suggests that there is no real internal consistence in the measurement. However, this factor is still retained as it emerges as a relevant offender decision-making factor in the interviews as well.

Table 10: Reliability Statistics

Cronbach's Alpha	N of Items
.571	3

Table 11: Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
BypassIDSEase_1	5.83	3.211	.388	.461
BypassIDSEaseNetworkDetectionSystem_1	5.86	3.063	.414	.421
BypassIDSEaseHostIDS_1	6.27	2.871	.347	.532

Thus, three factors are retained for the Preventative category, namely ‘protection updates’; ‘security testing and vulnerability assessment’; ‘ease of bypassing IDS’. The process above is repeated for the remaining SPAAR groupings [Appendix D]. The factors for each of these groupings are listed in Table 12:

Table 12: EFA 'Pre-Attack' Factors

Grouping	Retained Factors
System	Network security & monitoring; Lack of redundancy; Non-cyber/Physical access; Remote Access; Authentication
Preventative	Protection updates; Security testing & vulnerability assessment frequency; Ease of bypassing IDS
Attacker	Commercial; Political; Leisure; Business-Financial
Attack	Information-seeking techniques; Installation techniques; Non-technical techniques; Attack-in-progress techniques
Result	Human health; Information; Environment & health; Order & finance; Plant operations

Surveys offer one means of identifying factors influencing offender decision-making. As noted earlier though, the items in the survey are strictly informed by existing literature, which is mostly technical in nature. There may be other factors that are not addressed in the technological domain, particularly the human component of critical infrastructure cyberattacks. The interview therefore complements and supplements the survey as it has the potential to identify new factors or add more depth to the EFA-retained factors. Two main coding categories form the basis of the thematic analysis: Offender and Target.

Three offender-related factors emerge: resources; organization; and attacks. Three main types of resources arise from the data, namely skills, money, and time. These resources are considered to be crucial for the successful planning and execution of ICS cybercrimes:

> "if anything, some **very very good virus writing**, but more importantly … **a very very very deep understanding** of the vulnerabilities for that system, how to exploit those vulnerabilities, how to do things with a payload …" – *Hacker 2 (Skills)*

> "From a monetary investment, zero days go on the black market, for Windows O/S – for about 100K, give or take. About **$100,000 for a single zero-day** with an exploit mind you. Ok. So they put **4 of them … Black Market value for a digital cert is b/w a 100K and 200K**… So what does that tell you? It tells you that it was funded. **Quite well-funded** in fact." – *Industry 1 (Money)*

> "To me, I would put it at skills, I'd put it at preparation time. I mean, this is **months worth of planning and preparation, this isn't just** a payable coding that's **done in a couple of weeks**. To me – that's really needed multiple months of preparation." – *Hacker 3 (Time)*

The second offender-related factor is organizational dynamics, namely alliances and division of labor. While some ICS attacks are committed by groups whose members know each other, other crime networks have anonymous sub-networks. However, anonymity does not impact organizational sophistication; a complex division of labor can still exist:

> "… I believe it was developed through some sort of **compartmentalized project where you had 2-3 people** who knew what the end-state was, with **a bunch of people working on a specific problem** and not actually knowing where the outputs of their efforts went…" – *Hacker 2 (Alliance)*

> "…this is not easy stuff. It was **definitely put together by a group** – unless one person is doing this and they are extremely good – I'd love to meet them I tell you! That'd be one hell of a person..." – *Hacker 3 (Alliance)*

> "**I don't think the (vulnerability) guys … knew the CS (control systems) guys**. I bet you they **didn't even know where their code was gonna go. I don't think they cared**. I bet you they got their $100K per vulnerability and bought a Chinese sports car – I don't know what they do with it. That would be my guess" – *Industry 1 (Alliance)*

> "So you've got a **malware guy**, who's coded the zero day, you've got a **command and control guy**, who's focused on creating command and control network… You also had at least **one CS engineer**… You had **somebody who knew the Siemens software inside and out**, and then you had typically – a **different guy – who knew the h/w platform inside and out**… **(roughly) six people** …" – *Industry 1 (Division of Labor)*

The third offender-related factor is attack properties, such as research and development and the technique itself. ICS attacks are often well-planned; the target is researched extensively to identify its properties and weaknesses, which are used to identify and design the most appropriate set of attack techniques.

> "If my goal is to … bring down a generation plant, … probably **50-75% of the legwork is to learn as much as I can** about that environment beforehand. Whether it be through **social engineering**, calling these people and trying to understand what systems operate in their plant… **Research the vendors and system and get my hands on a copy of the system**, understand what inputs and outputs it takes and what I can manipulate…" – *Hacker 1 (Research & Development)*

> "… a lot of the information that an adversary would actually need to target a specific facility or system is out there somewhere. It's **sitting on a DB, sitting in someone's email, on a laptop computer** … we have the technology to go out there and pilfer and get … all related information about the target actually … that could be **tweets, blogs, home information, photos, travel plans, anything**. The info about vulnerabilities, per se, can be obtained in several ways…" – *Hacker 2 (Research & Development)*

> "… we call it **packing, so we bundle up the s/w in a way that it's encrypted, so people can't see what it's designed to do**. … So by putting multiple layers, it's kinda like inception – "a dream in a dream in a dream" **packed inside itself several times**. So those are the different layers" – *Hacker 1 (Technique)*

Three target-related factors emerge: accessibility; prevention measures; and weaknesses. Two main types of accessibility avenues arise from the data: electronic and physical. As noted in the literature review, ICS are increasingly being connected online and to corporate networks for better efficiency; but this increased connectivity is abused by cybercriminals. This electronic access exploitation resonates in the interviews. The physical access component, however, is not evident in the literature and emerges as an equally important means of gaining entry to ICS:

> "we have now taken **previously secure system … (and) plugged it into insecure system** or worse, an actual corporation. You've **opened up those risks and those threats** ..." – *Hacker 3 (Electronic Access*)

> "And so we're basically **networking all these systems together** and becoming much more complex piece of equipment, which is a **much larger attack surface**" – *Industry 2 (Electronic Access)*

> "we **walk into companies 'hi I'm xxx – I'm from xxx – we're here to fix computer system" – "oh not a problem – here's our data center" – "thanks guys, buh-bye now**" – you know it's that bloody simple to get into a company… **Do you have to be sophisticated if you have to [physically] break into** … their headquarters, which might have the monitoring of that facility plugged into their corporate network – **no it's a piece of cake**." – *Hacker 3 (Physical Access)*

One of the main issues concerning prevention measures is whether they exist, and if so are they effective. Another issue is that if the industry needs to introduce protection measures or install security patches, they often lose vendor support. Finally, attacks are rarely detected in real-time; most attacks are discovered well after the attack ends:

> "you look at the energy industry, - we keep building these damn things, and **we don't actually necessarily do anything about protecting the CS**" – *Hacker 3 (Quality/Existence)*

> "the **poor management of the system, the poor ability to monitor the systems**, those make the ICS environment very very juicy from an attack perspective" – *Industry 1 (Quality/Existence)*

> "The problem again is that this goes back to the vendor who says 'well, hey – **we won't support your system unless you were at this version**', and well that version is vulnerable to an attack, so what are we supposed to do, so you have to find **different mitigations or risk, becoming unsupported by the vendor by putting a host of firewalls into your system**" – *Hacker 1 (Vendor Support)*

> "I'll take a very pessimistic view on this one. The industry is **effectively blind**. And I think that's a fairly accurate assessment… **logging and reviewing logs** both at the perimeter and the critical cyber assets w/i those perimeters. But … the capabilities to do that are **fairly limited**… **the sophistication of the tools to do the analysis and the human resources that are thrown at that problem are typically fairly minimal**. … the

> first indication that someone's gonna have that they've been **compromised is when something breaks**." – *Industry 3 (Detection)*

The third set of target-related factors, system weaknesses, includes two main issues. First many vendors use commercially available software to cut production costs, which increases ICS susceptibility. Second, ICS architecture is slow to change and adapt, which makes studying the target and designing the attack easy for cybercriminals. Third, the introduction of updates is a slow process, and the frequency/quality of testing these updates is poor or nonexistent.

> "Vendors … maximize the efficiency of their systems but reduce the overall cost by … **using commercial available O/s (operating system) … they wouldn't build their own asset anymore**. This gets very interesting b/c you now introduce a whole slew of **known and specific o/s vulnerabilities** that if capitalized on will have a very good impact… And that becomes very attractive" – *Hacker 2 (COTS)*

> "… the deterministic and somewhat **static nature of architects – these systems don't change**. The same thing all the time. They're running power, making power, distributing power – that's great. That … is an adversarial dream … the **reconnaissance system that you're looking at day 1 is identical to the system that you're looking at day 1500. That gives you lots of opportunity to go under the radar**, and that's great for an adversary." – *Hacker 2 (Architecture)*
> "You got to remember the **uniqueness** of this technology that's available – these **systems are 25 years old** and they're running the infrastructure. You can **buy them for a fraction of a cent on the dollar on eBay. You buy it, you break it, you post it**. There are hundreds, hundreds, many hundreds of vulnerabilities on SCADA and CS technology specific to the power sector, water sector." – *Hacker 2 (Architecture)*

> "… for most CS, **the introduction time frame for a new item of s/w is umm… the earliest at about 3 months, typically is 6 months, 12 months are not unusual**… you don't want the change … to cause more harm than the change you were trying to defend against. [Updating]… is a pretty **slow process**, and only in the rarest case does it happen in less than 3 months… pressure from some of the larger utilities, **some vendors do testing**. Vendor industry is very **immature … and their testing is not particularly effective… Some of the vendors don't do any testing at all.**" – *Industry 4 (Updates/Testing)*

These factors (summarized in Table 13) influence offender decision-making in the pre-attack stages. Once the attack commences, however, different factors may emerge (industry reaction, unanticipated situation), which also impact the offender decision making process.

Table 13: Interview Analysis 'Pre-Attack' Factors

Theme	Sub-theme	Further sub-themes
Offender	Resources	Skills; Money; Time
	Organization	Alliance; Division of Labor
	Attacks	Research; Technique
Target	Accessibility	Electronic; Physical
	Prevention	Existence/Quality; Vendor; Detection
	Weaknesses	COTS; Architecture; Updates/Testing

Hypothesis 5: The factors that impact offender decision-making processes also emerge from the attack-in-progress environment, and include attack techniques, target responses, and exploitable weaknesses.

As noted earlier, the analysis results are based on hacker and industry *perceptions*; the factors that influence offender decision-making are therefore based on indirect perceptual data, which should be interpreted tentatively. The remaining SPAARR factor (Reactive) is used to test this hypothesis. The EFA for this factor can be found in Appendix D. Additionally, other post-attack factors emerge from the interview analysis, which are broadly grouped under dynamics-related factors: cost-benefit analysis; response; counter-response; and exit. All hackers agree that a well-structured attack plan is needed to target ICS. Furthermore, the attack plan has to account for all possible scenarios as the crime progresses so as to increase its success rate. Thus, the attack plan has both preconceived and dynamic decision trees:

> "My thought process is from a **cost-benefit analysis** is that I am going to always follow, directly or indirectly, the **hacker wheel because of reconnaissance system, privilege escalation, explore more systems, cover my tracks**, all of this kinda stuff." – *Hacker 2 (Attack Plan)*

> "First I've figured out **what ports I can get on**, I've figured out **what IDs and what passwords I can use** to get into the infrastructure if I need those, I've figured out **how I'm going to come in**, I've figured out where I'm going to come in now, figured out **how do I control whatever's going on** – am I leaving something behind that's going to report to me …" – *Hacker 3 (Attack Plan)*

> "… the attack plan will be comprised of **branches and sequels … at each point of penetration and attack** in the system" – *Hacker 2 (Decision Trees)*

The industry typically has three main responses to an attack. It can isolate the targeted system to prevent the attack from spreading. It can engage in attack source and methodology reconnaissance by leaving the attack running. Finally, the industry can feed the adversary false data to thwart the attack:

> "There's a general best practices strategy, where you **identify the fact that you've been targeted, isolate the systems, eradicate the infection, and then recover the system to a pre-infected state**. Except that the one minor difference is that you hopefully mitigate the vector that was attacked in the first place." – *Hacker 1 (Isolation)*

> "… **leave that attack running to learn and gain more insight and intelligence** on exactly what the heck is going on… We actually watched an attacker get in … you're monitoring, you're watching, you're seeing what they're doing, you're basically **learning what the attacker's methodologies are**. And you're also trying… to **figure out who the heck it is** that is doing it. The **longer you leave it running, the better potential chance you have of finding out who the hell's doing it**" – *Hacker 3 (Reconnaissance)*

> "You **start feeding it false data or false information**, you can sometimes [see] if **it's reporting back onto an IRC channel**, what information can you feed back there… you [can] potentially **feed your own payload in file back to those guys and start tracking that back**…." – *Hacker 3 (Feed False Data)*

The third set of Dynamics-related factors deals with the how cybercriminals respond to industry reactive measures. There are two main types of counter-responses. First, cybercriminals find alternate means of access, if the system they target is isolated. Alternatively, adversaries adapt by changing their attack tactics:

> "If I'm an attacker, and if I was a smart attacker, I would usually have **second or third channels, or paths back into the infrastructure** … that (has) been compromised that would give me other means. And so if one of these systems had been isolated I would then try to **go through and gain control to one of the other systems**." – *Industry 2 (Alternate Access)*

> "So if the adversary can't get in remotely … the **tactics absolutely have to change**, and that could be **physical penetration**, it could be **penetration into assets that are connected … to the network but not necessarily … to the outside world**, and things like that" – *Hacker 2 (Alternate Tactic)*

The last set of dynamics-related factors deals with exit strategies, which can be used either when the attack is complete or when the adversary has been exposed. Two main strategies are used. First, cybercriminals remove any evidence that indicates their presence in the targeted ICS. Second, cybercriminals complicate the digital trail back to them, which allows them to remain unknown and continue their attacks:

> "When you get in to the system, you want to try and **delete the evidence** of what you did to get in, and **not leave things in there such that it's easy to detect your presence** when you're there or breaking in" – *Hacker 1 (Delete Evidence)*

> "…**so I'm going to make my trail to me and from me as complicated as possible**… what detection controls are in place? Are they monitoring their network, and if so, **how do I disguise myself so that I can go in there as benign traffic and I don't have a pattern** …" – *Hacker 3 (Tracking Complexity)*

The factors obtained via EFA and interview analysis are summarized in Table 14 below:

Table 14: Combined EFA & Interview Analysis 'Attack-in-Progress' Factors

Theme	Sub-theme	Further sub-themes
Dynamics	Cost-Benefit Analysis	Attack Plan; Decision trees
	Response	Type: Isolation; Reconnaissance; Feed False Data Body: Industry; Public-private; National; International
	Counter-response	Alternate access; Alternate tactic
	Exit	Delete evidence; Tracking complexity

Reviewing PARE RISKS

The exploratory factor analysis (EFA) and interview analysis each yielded several factors that influenced offender decision-making. What did this imply for the original PARE RISKS framework? Was it an adequate framework? Each of the factors retained through the above analysis can easily be mapped to the nine from the original framework as shown in Table 15 below. It is important to note, however, that many of the elements originally included for each PARE RISKS factor did not emerge in the analysis. EFA sifts through the original PARE RISKS elements and condenses them into a new set of factors. Thus, despite the clean mapping back to PARE RISKS framework, some of these factors now have fewer items. For instance, the 'Response & Recovery' factor is now simply 'Response'; the 'Recovery' component does not seem to impact offender decision-making processes. Nor did this component emerge in the interview analysis as a relevant factor that influenced how offenders made decisions.

There are also some additions to the original framework, such as the physical access to ICS, which indicates that even though the mapping is successful, new elements are still being incorporated into the original framework. Other new elements were 'Crime Dynamics' factors, such as using alternate access and techniques in response to industry reaction. Another new Crime Dynamics factor is the offender's need for well-designed attack plans that consider all possible situations (decision-trees). This plan can be used to manage an industry response and continue with the attack. Finally, the Exit strategy is also a new addition to the PARE RISKS framework. Offenders can delete any logs or evidence that can be traced back to them, and they can also hop through several transit ports in cyberspace to mask their digital footprints. Thus, even though the PARE RISKS framework still accounts for the revised set of factors, there are some modifications.

Table 15. Revisiting PARE RISKS

PARE RISKS	
Prevention Measures	• Protection updates • Ease of bypassing IDS • Existence/Quality • Vendor-based • Network security & monitoring
Attacks & Alliances	• Attacker Type: Commercial; Political; Leisure; Business-Financial • Organization: Alliances; Division of Labor • Attack Technique: Information-seeking techniques; Installation techniques; Non-technical techniques; Attack-in-progress techniques • Resources: Skills; Money; Time
Results	• Data Modification; Plant Operations
Ease of Access	• Electronic/Remote; *Physical* • Weak authentication
Response ~~and Recovery~~	• Type of Response: Isolation; Reconnaissance; Feed False Data • Responding Body: Industry; Public-private; National; International • *Counter-response: Alternate Access; Alternate Tactic* • *Exit Strategy: Delete Evidence; Tracking Complexity*
Interconnectedness & Interdependencies	• Human Health; Environment; Civic Order; Finance
Security Testing, Assessments & Audits	• Security testing & vulnerability assessment frequency
Knowledge, Skills, Research & Development	• Research & Development • *Attack Plan* • *Decision Trees*
System Weaknesses	• COTS; • Architecture/Legacy Systems • Inadequate Redundancy

* *New items are italicized*

Strengths and Limitations

This study is important because it initiates a discussion between multiple domains: ethical hacker base, electricity industry, and criminal justice. Hackers share the same skill set as cybercriminals and therefore offer relevant insight into exploitable ICS vulnerabilities. Industry experts have insider information on (undisclosed) power sector cyberattacks, which sheds light on ICS weaknesses and cybercrime prevention measures. Offender decision-making, however, is a multi-faceted process that not only assesses target suitability and capable guardianship, but also assesses the resources available to the offender. Drawing on criminology theories that account for offender decision-making offers a more plausible take on ICS cyberattacks. This study, while small-scale in scope, serves as a collaborative effort by bringing together a diverse set of people with different views, objectives and knowledge to address a common problem. This preliminary collaborative approach enables 'big picture' thinking about ICS cyberattacks.

This study is also significant from a methodological perspective. It employs a systematic mixed-method procedure to explore factors that influence offender decision-making. It surveys 322 hackers and industry experts to identify their ICS TVC perceptions. Though this study is exploratory in nature, it uses a novel approach to examine ICS cyberattacks. It simultaneously compares industry and hackers using the same survey instrument. This method can serve as a guideline for future studies directed at cyberattacks against other critical infrastructures; it can be tailored to reflect the corresponding sectors. There are, of course, methodological limitations to this study, which are discussed next.

Surveys: Surveys offer several advantages. First, they offer speed, cost, and flexibility advantages. Questionnaires are quick and easy to complete by respondents. The costs involved once the initial setup is complete are minimal and large sample sizes do not cost more than smaller ones. Second, surveys often generate more honest responses on sensitive topics, such as drug use or sexual practices, as participants feel more comfortable giving their answers anonymously on paper than in-person to a researcher (surveysystem.com 2009). Therefore this method is appropriate to study the sensitive topic of ICS TVCs. Finally, surveying both hacker and industry populations offers a means of cross-checking the concept of TVCs; this strategy permits searching for regularities in the collected data and offers a more detailed and balanced picture electricity ICS TVCs (Denzin 1978b; O'Donoghue & Punch 2003).

A problem with surveys is selection bias, which occurs when subjects are not representative of the target population about which conclusions are to be drawn (BMJ.com 1997; Shadish et al. 2002). In this particular context, survey respondents in both domains may not have the knowledge necessary to complete the survey; they may be unaware of all possible threats and vulnerability assessments, and may also possess varying levels of technical expertise. This limitation, however, cannot be avoided given the exploratory nature of this research. One means of handling this shortcoming is to compare the survey responses with technical vulnerability assessments conducted by industry, which is discussed in the 'Discussion' section of this chapter.

Bias can also be introduced into the study given the different survey administration techniques. Research on difference in response rates for online surveys

compared with traditional surveys is mixed, with studies showing higher, lower, or similar response rates (Lonsdale et al. 2006). All 202 hacker surveys are paper-based. Industry surveys are done both in online and paper formats; only 12 surveys are internet-based and 109 are paper-based. Comparing online and paper-based industry responses do not reveal any significant differences.

Reliability is concerned with how accurately any variable is measured (King & Horrocks 2010). The PARE RISKS factors are identified through the literature. However, there may be other factors are not disclosed in the existing literature and therefore are not reflected in the surveys. Additionally, some factors are over represented, such as system weaknesses and preventative measures as this is predominant in the literature. Therefore these factors have more survey items, which impact the factors that are retained through exploratory factor analysis. Furthermore, this over-representation can also affect the corresponding Cronbach's α, which is a measurement of item-scale reliability. The value of α depends on the number of scale items (Cortina 1993). Therefore as the number of items on the scale increase, α also increases. So it is possible to get a large value of α because there are a lot of scale items and not because the scale is reliable. However, the best possible offender decision-making factor set is identified for this exploratory study. Furthermore, while reliability is an important factor in survey research, it is particularly so in the case of inferential statistics, which is not used here.

Response rate is also an important indicator of how much confidence can be placed in the results of a survey. A low response rate, given the sensitive nature of this topic, decreases the reliability of the proposed study (Maxfield & Babbie 2005). This problem of low response rates is tackled by advertising through both hacking and

industry communities prior to administering the survey to increase the response rate (Cook et al. 2000). As noted earlier, the survey was advertised with DEFCON, NERC, SANS, SCADASEC, and ENERGYSEC to increase its exposure and obtain multiple avenues for accessing respondents.

Interviews: The criterion most often required for sampling in qualitative research is diversity; participants who represent a variety of positions in relation to the research area (King & Horrocks 2010). The effectiveness of such a sampling strategy, however, depends on the choice of categories from which to select participants. This choice depends on a combination of the researcher's knowledge of the categories, personal knowledge, and anecdotal information from those who either participate in, or have some involvement with, ICS security issues (King & Horrocks 2010). Given the sensitive nature of this topic, complete knowledge of the various types of individuals such as, security testers and auditors, ICS operators, ICS vendors, and electricity sector management, is difficult to obtain. Wherever possible, however, diversity is incorporated while recruiting subjects. For instance, participants had experience in testing ICS, extensive experience with electricity sector ICS, and were involved in designing ICS audits and security policies.

This study conducts interviews over the phone. Some disadvantages have been noted in past research with regards to using phone interviews instead of face-to-face interviews. First, there is greater difficulty in achieving rapport, and the lack of visual cues hinders the interpretation of speech (as cited in Carr & Worth 2001; King & Horrocks 2010). A second disadvantage relates to the limitations placed on the length and complexity of the interview, with "20 to 30 minutes being considered the maximum

before respondent fatigue sets in" (as cited in Carr & Worth, p. 514). A third limitation is that phone interviews produce shorter responses than face-to-face interviews. Fourth, there is an inherent role imbalance in phone interviews, where the "caller has the initiative and the answerer must react" (as cited in Carr & Worth, p. 515). While these limitations are of concern, they are overcome in several ways. First, the respondents are provided with a research abstract, assent form, and interview guide that outline the details of this study. They are also provided with information about their rights as research participants and contact information of the researcher and the Rutgers University ethics committee. Finally they are also aware of what questions to anticipate. This strategy prevents participants from receiving any unforeseen surprises during the interview and they know what to expect. In some instances, the participants add their own thoughts and even expand the set of questions, which results in a richer interview. Contrary to the second and third limitations listed above, respondents are eager to speak over the phone, resulting in interviews that range from 90 to 105 minutes in duration, which offers in-depth responses. Initial questions comprise the background questions, which are straightforward and simple, help increase respondents' sense of competency, and reduce any anxieties.

Other factors contributing to the richness of phone interview data can be contributed to the relative anonymity of the medium itself, the complete anonymity guaranteed to the participants, and asking questions about their perceptions alone without discussing specific cases, which collectively makes it easier for subjects to speak freely. Regarding role imbalance, the phone interview gives the respondent the freedom to answer without placing any time and content restrictions; the interview is designed to be

informal and conversational in style, which allows respondents to answer to the best of their ability. Furthermore, early open-ended questions help establish rapport and allowed participants to 'find their voice' (as cited in Carr & Worth 2001). The above discussion illustrates that some of the survey and interview limitations identified in the literature are irrelevant to this study. It also demonstrates how some of these limitations are managed. Having addressed these limitations, the next sections summarize and discss the findings of this research.

Summary of Findings

The 'Introduction' chapter listed ten research questions that relate to offender techniques, alliances, information sharing, resource availability, management of industry responses, and the factors in pre-attack and attack-in-progress environments that influence offender decision-making. The research findings are organized around these ten questions, which are summarized in Table 16 following the discussion below. It is important to remember that the findings below are based on hacker and industry *perceptions* and not on any direct data, and as such should be interpreted tentatively. However, the 'Comparing Perceptions and Reality of ICS Cyberattacks' discusses this issue and reveals several parallels between this perception study and actual technical ICS assessments conducted by industry.

1. How do cybercriminals select suitable ICS targets?

   Cybercriminals use two main avenues to research their targets. First, they study their targets by researching ICS vendors and system blueprints, which can be obtained through several ways, such as accessing databases, emails, and laptops, and viewing

blogs and tweets (professional or personal webpages). Second, social engineering strategies can be used, where offenders use human interaction, or social skills, to obtain and/or compromise information about an organization's computer systems. These offenders may seem unassuming and respectable; however, by asking questions, they can piece together enough information to gain knowledge about their target.

2. What techniques do cybercriminals use to implement ICS attacks?

   There are four main types of techniques used: information seeking, installation, non-technical, and attack-in-progress. First, information-seeking techniques are typically used in the preliminary stages of the attack to learn more about the target. Second, installation techniques are how particular attack vectors are introduced to the ICS in question. Third, non-technical strategies are also used, such as social engineering and pre-written toolkits. While social engineering is used to obtain background information, it also provides the means to get access to an ICS. Attack-in-progress techniques, such as data manipulation and compromise, occur once offenders penetrate their targets – these techniques permit offenders to achieve the desired consequence of their attacks.

3. Do cybercriminals form alliances for ICS cyberattacks? What is the nature of these alliances?

   Cybercriminals can form alliances to engage in ICS cyberattacks. There may be a small group of associates, or organizers, who oversee the entire criminal plan and may delegate smaller, sub-tasks to other individuals or compartmentalized groups. These group members may not know what their particular end-product will be used

for. They may be unaware of the overall group size, other groups involved, and other malicious software being produced. Thus, there appears to inter-group anonymity with regards to member identity and tasks. Finally, each group is autonomous; it completes and delivers its finished product to the organizers, who then correspond with another compartmentalized group.

4. If alliances between cybercriminals exist, is there a division of labor?

   The compartmentalized organization based on knowledge and skills suggests that a division of labor is employed. The data suggests that an assortment of expertise is required in ICS hardware and software platforms, command and control, writing malware, and testing and quality checks. Depending on the expertise and knowledge, the same individual(s) can have overlapping tasks.

5. What types of resources are available to offenders? How do the availability and quality of these resources impact the attack process?

   Cybercriminals need *enough* skills, money, and time to engage in ICS cyberattacks. Some of these skills have been addressed for question 4 above. A very deep understanding is necessary to understand the target, its weaknesses, and design appropriate attacks. ICS cyberattacks can be very expensive (ranging from $100,000 to $600,000), which suggests that they are well-funded. Planning, designing, implementing, and testing these attacks are time-consuming, requiring several months. Though these three resources are important, their availability level is also crucial. Thus, if an organization has the necessary skills, money, and time, but eventually runs out of one (or more) of these, the cyberattack cannot continue. The

data suggests that state-sponsored ICS cyberattacks have unlimited access to skills, money, and time, resulting in continuing cybercrimes against the electricity industry.

6. What are the possible consequences of an ICS cyberattack?

   There are two types of outcomes: direct impacts on the electricity sector itself and indirect impacts on other dependent infrastructures. Direct impacts include modifying sensitive information or data that affects data-dependent decisions (replacements and patches). Another direct impact involves altering input/output of SCADA or PLCs, which affects plant operations. Four indirect impacts on other infrastructures emerge from the data. First, finance may be affected; disrupting electricity may affect transactions, transfers, ATMs and electric-based security mechanisms. Second, civic order can also be affected – the disruption of electricity services can disrupt day-to-day activities, offices, and commercial enterprises. Third, the environment can also be impacted; disruption of the electric grid serving water and sewage infrastructures can cause waste spillage and contamination. Finally, human health is also affected; emergency services, hospitals, and water are all vital human health sectors that rely on electricity.

7. Which institutions respond to ICS cyberattacks? What are some response strategies?

   Four types of institutions respond to ICS cyberattacks, and these are not in any rank order. First, at the international level, are the Central Intelligence Agency and Secret Service. Second are the national-level responding bodies, namely the Department of Homeland Security and the Federal Bureau of Investigation. The third type of response is from the public-private arena, with local police departments and private

security firms. The industry also has its own means of responding to cyberattacks. Three main response strategies are used either separately or collectively. First, the infected ICS is isolated, repaired, and restored to its pre-infected state. The second response is to leave the attack running to gather information about the attack source, technique, and goal. The third response involves feeding false data back to the offenders to mislead them, which can reveal their next course of action.

8. How do cybercriminals handle industry responses and evade detection?

   Cybercriminals have two counter-responses. First they can use alternate techniques, such as a different type of malware and physical penetration. Second if the industry isolates the targeted ICS, cybercriminals can use alternate paths or channels to target other ICS components. Cybercriminals have two strategies to evade detection. First, they delete all access logs or any other evidence that reveal their presence. Second, they make their digital trails as complex as possible and avoid creating patterns.

9. What are the pre-attack factors that influence offender decision-making?

   Cybercriminals must first do their research, acquire resources, form necessary alliances, select targets, and design attacks (questions 1 through 5); these are all pre-attack factors. There are other factors that also influence offender decision-making before initiating a cyberattack. First, cybercriminals must gain access to the system, which is possible in two ways. They can gain electronic access via exploiting weak authentication systems and overcoming network security and monitoring. Alternatively, they can gain physical access to the system by entering corporate offices that have poorly protected remote ICS access.

Second, they must bypass any prevention measures, such as intrusion detection systems. Cybercriminals benefit from poor prevention practices, such as poor system management and minimal resources invested in real-time detection. Cybercriminals can also take advantage of the slow ICS-vendor software development cycles. If the current version of ICS is vulnerable to cyberattack, and the industry installs a readily available patch, it may lose vendor customer support for that version. The industry may therefore wait for the next ICS version which fixes that vulnerability, but risk having that vulnerability exploited till moving to the next version.

Third, cybercriminals must exploit system weaknesses. Vendors use commercial software to maximize system efficiency and reduce overall costs, but this software has known vulnerabilities that cybercriminals can easily exploit. ICS systems do not have enough redundancy in their designs; cybercriminals can exploit this architectural flaw knowing that the industry has fewer backups in place to continue operations. ICS systems are 'legacy systems' because they have not changed in the past 25 years. Their vulnerabilities are well-known and do not change easily or quickly. Cybercriminals can plan and design their attacks knowing the rather static nature of ICS. Vendors and industry do not engage in frequent good-quality security assessments, which may reveal vulnerabilities that cybercriminals can exploit.

10. What are the attack-in-progress factors that influence offender decision-making?

Offender decision-making also exists after the cyberattack is initiated; several attack-in-progress factors are relevant. Cybercriminals constantly engage in a rational, cost-benefit analysis to ensure that they follow the path of least resistance. They have a strategic attack plan complete with decision trees that capture as many potential

scenarios they can think of. These scenarios may cover industry responses to the attack (question 7: isolation, reconnaissance, feed false data) and possible counter-responses (question 8: alternate access, alternate tactics, exit strategy).

Table 16: Summary of Findings

Research Question	Findings
1. Target Selection	1. Knowledge Acquisition: *Databases, email, laptop, tweets, blogs, home information, travel plans* 2. Social Engineering: *Research members of IT department, physically visit plant, Phone calls with fake credentials*
2. Techniques	*1.* Information-seeking: *System scan, IP Spoofing, spyware, toolkit, information theft, script fuzzers/brute force attack, and use as distribution system* *2.* Installation: *Viruses and worms, malware, and spyware* 3. Non-technical: *Toolkits, social engineering* *4.* Attack-in-progress: *Data manipulation, physical attack, and information compromise*
3. Alliances	*1.* Compartmentalized groups: *Sub-groups based on specific tasks* *2.* Anonymous: *Sub-groups do not know other sub-groups* 3. Autonomous: *Each sub-group works independently of other sub-groups*
4. Division of Labor	1. Knowledge & skills: *ICS engineer, software platform, hardware platform, malware, command and control, testing and quality assurance* 2. Overlapping tasks
5. Resources	1. Skills: *ICS engineer, software platform, hardware platform, malware, command and control, testing and quality assurance* 2. Money: *$100,000-$600,000* 3. Time: *Weeks, months, or years* 4. Availability: *(un)limited*
6. Consequence	1. Direct: *Modifying data/information; tampering plant operations* 2. Indirect: *finance, civic order, environment, health*
7. Response	1. Agency: *International, national, public-private, industry* 2. Strategy: *Isolation, reconnaissance, feed false data*
8. Manage Industry Response	1. Counter-response: *Alternate access paths; alternate techniques* 2. Evade detection: *Delete evidence; complex trails*
9. Pre-attack Factors	1. Factors 1-5 above 2. Accessibility: *Electronic, Physical* 3. Prevention: *Security, Vendor* 4. Weakness: *Commercial software; poor/infrequent testing and assessments*
10. Attack-in-progress Factors	1. Factors 7 & 8 above 2. Cost-benefit analysis: *Path of least resistance* 3. Attack plan/Decision Trees: *Potential situations with solutions*

Comparing ICS Cyberattacks Perception and Reality

This study is exploratory in nature and based on hacker and industry *perceptions*. As such, there is concern on whether perceptions are reflections of reality; does the revised PARE RISKS framework, which is based on industry and hacker perceptions, parallel actual cybersecurity studies? Does this framework contribute to industry vulnerability assessments, and if so, how? Two industry assessments serve as comparison points. The first report is on electricity ICS cybersecurity assessments conducted by the Idaho National Laboratory (INL), which seeks to identify vulnerabilities that could put critical infrastructure at risk from a cyberattack. This report presents five results from 24 ICS assessments from 2003 through 2009 (INL 2010). First, excessive unsecure open ports increase the ICS attack surface (INL 2010). Second, well-known unsecure coding practices result in several ICS software vulnerabilities, which in turn, result in increased system access (INL 2010). Third, poor patch management practices are more likely to cause ICS attacks because these patches are for known vulnerabilities that potential offenders can exploit via easily available attack tools (INL 2010). Fourth, perimeter defenses are not enough; vulnerabilities in web services, database applications, and data transfer protocols all offer attack paths through firewalls (INL 2010). Fifth, weak authentication and integrity checks allow unauthorized ICS access and control (INL 2010).

The second assessment is by the US Department of Homeland Security (DHS) National Cyber Security Division's Control Systems Security Program (CSSP). This report offers 18 security assessments of new ICS products and production ICS installations from 2004 to 2010 (DHS 2011). This report has four results. First, poor

access controls and weak network design, such as weak or non-existent firewall rules, increases ICS access (DHS 2011). Second, authentication (permissions, privileges, and access controls) is often weak (DHS 2011). Third, the lack of formal documentation on proper installation, updates, and patches also increases ICS susceptibility (DHS 2011). Fourth, the delay in vendor patches prevents ICS asset owners from using other patches as they may lose vendor support (DHS 2011).

Both these reports are based on actual ICS cybersecurity assessments, the former focusing on electricity sector ICS and the latter conducting a more general ICS assessment. This perception study parallels both the assessment studies well. Increased access and connectivity, poorly protected networks, weak authentication protocols, and infrequent security and patch updates are all findings that also emerge from this study. However, as noted in the 'Introduction' chapter, the INL and DHS assessments are mostly technical in nature. Routine Activity Theory (RAT) states that three elements must coincide in space and time for crime to occur: likely offender, suitable target, and capable guardian. These technical assessments focus on the second and third elements of RAT. This study, however, makes the case that the first element should also be considered to get a fuller picture of ICS attacks, which requires moving beyond the technical knowledge base.

First, ICS attacks do involve human (offender) aspects as well, such as available resources and target-specific research, which can be *non-technical*. The capable offender can engage in non-technical social engineering tactics, which trick legitimate insiders into divulging sensitive ICS information. ICS documentation and blueprints are often found online, which cybercriminals can use to extensively study their target and design tailor-

made attacks. Also, offenders can physically access corporate networks, which may bypass firewalls and connect directly to ICS. These issues, though non-technical, may contribute to the occurrence of ICS cyberattacks, yet are not fully addressed in cybersecurity assessments.

Second, this research illustrates the dynamic nature of ICS cyberattacks by focusing on both pre-attack and attack-in-progress environments. Identifying which offender decision-making factors are relevant at both these stages is essential to designing pre-attack *peripheral* prevention measures, *internal* ICS prevention measures, and attack-in-progress *reactive* measures to generate the strongest and most successful defense mechanisms. Doing so deters the capable offender by increasing the costs involved in continuing with the attack. Having discussed these issues, several implications can be drawn for cybersecurity practice, which are addressed in the next chapter.

Chapter VI. Conclusion

This research explores hacker and industry perception gaps on threats, vulnerabilities, and consequences (TVC) to determine how these gaps can inform better prevention and security practices. Furthermore, it identifies a set of offender decision-making factors that come into play when cybercriminals target electricity sector ICS. This chapter first identifies implications for theory by evaluating the effectiveness of RAT and RCT based on scope, coherence, and explanatory capacity. It then discusses some unexpected, yet interesting, findings on crime processes or scripts and the notion that decision-making factors are interactive. These findings suggest that RCT should be supplemented by Game Theory, which may be useful to address how offenders make decisions about target selection, attack technique, strategy modification, attack dynamism, and apprehension evasion. Next, this chapter outlines some implications for practice, such as consistently using standard definitions, designing education programs, and using mandatory security budgets. Finally, the chapter concludes with several ideas for future research, such as using different methodological approaches to further identify offender decision-making factors, using agent-based modeling and simulation exercises to determine decision-making factors in ICS-like settings, and using situational crime prevention principles to better inform cybercrime prevention practices.

Implications for Theory

This research employs well-established offender decision-making theories for analysis, namely rational choice theory and routine activities theory. These theories are

used to understand the offender decision making process during ICS cyberattacks. Theories can be evaluated on the basis of their scope, coherence, and explanatory capacity. Wagner (1984) and Shoemaker et al. (2004) state that theories should be evaluated on the basis of scope, or the comprehensiveness of the account of a particular problem. One means of determining the comprehensiveness of theories is to compare them with observations. This research uses survey and interview *perception* data to assess the relevance of RCT and RAT. The five research hypotheses are supported, indicating that cybercriminals are perceived as engaging in a cost-benefit analysis by evaluating their criminal environment. If a suitable ICS target is available without the presence of a capable guardian, the potential offender targets the ICS. Thus, a probable and comprehensive picture of the nature of ICS cyberattacks and offender decision-making is attained using RCT and RAT.

A theory is internally coherent if its concepts rationally interconnect with, and do not contradict, each other; concepts should be "logically related, build on each other, or contribute to the explanatory power of each other" (Swenson 1999, p. 2). The concepts put forth by RAT and RCT certainly do not contradict each other; they complement each other to suggest a reasonable picture of cybercriminal decision-making in ICS cybercrimes. Offender decision-making cannot be explained by a single concept; the concepts of 'suitable target', 'absence of capable guardianship', 'likely offender', 'cost-benefit analysis', and 'bounded rationality' are logically related as each cannot be explained without the other while accounting for ICS cyberattacks. Indeed, these concepts and theories are rationally connected and contribute to each other's explanatory capacity.

As Einstadter and Henry (1995) note, the "purpose of all theory is to understand and explain" (p. 12). Both RCT and RAT offer an explanation for how cybercriminals rationalize target selection and engage in cost-benefit analysis. This theoretical framework employs an interactive causality model of causal explanation, where factors ('capable offender', 'suitable target', 'absence of capable guardianship', 'decision-making') influence each other, such that crime and criminality are an outcome of this interactive process (Einstadter & Henry 1995, p. 15).

Game Theory

Interviews were used to fill out gaps in the survey data and identify any offender decision-making factors that had not been addressed in the surveys. While the interviews certainly supplemented the surveys, they also revealed unanticipated, but important, information on the crime process or script. Crime scripts identified every stage of the crime-commission process and the decisions and actions that were needed at each stage. Five distinct stages of the crime script emerged from the interview data, which are summarized in Figure 2 following the discussion below:

Stage 1 – Preparation: "… 50-75% of the legwork is to learn as much as I can about that environment beforehand. Whether it be through social engineering, calling these people and trying to understand what systems operate in their plant, or seeing if I can get hold of someone who doesn't like their job there and maybe convince them 'hey come work for me and tell me about what you used to do there'… Basically, you want to understand the system as much as you can and get a picture of the whole… From there, I'm going to take what I have and do as much research about the knowledge that I've gained. Research the vendors and system and get my hands on a copy of the system,

understand what inputs and outputs it takes and what I can manipulate… There's just going to be a whole lot of vectors and I'm going to try to take the one that makes the most sense and most likely to succeed." – *Hacker 1*

"… a lot of the information that an adversary would actually need to target a specific facility or system is out there somewhere. It's sitting on a database, sitting in someone's email, on a laptop computer – whatever it is… if we know what we're looking for, we can well-beyond web-crawlers and stuff, we have the technology to go out there and pilfer and get any and all related information about the target actually is – that could be tweets, blogs, home information, photos, travel plans, anything… you got IRC and chats over there where people are swapping this stuff, Left, Right and center… The info about vulnerabilities, per se, can be obtained in several ways." – *Hacker 2*

Stage 2 – Entry: "…you have to look at what methods of entry as well as what methods of exit, if it's physical or virtual, and again if it's physical and virtual – you have to look at the monitoring around it, the management around it, what controls are around it, how often is it being monitored, etc. Obviously ingress and egress points … especially ingress points." – *Hacker 3*

Stage 3 – Initiation: "I've figured out how I'm going to come in, I've figured out where I'm going to come in now, figured out – how do I control whatever's going on – am I leaving something behind that's going to report to me or am I going to be risking the fact that I'm in there for an extended period of time manually doing this." – *Hacker 3*

"…to get on a corporate network of a large facility … get a foothold on a desktop, so you got to try to convince somebody to click on a link or open a file that would then result in your specific piece of malware being installed on this computer. That would provide you

a backdoor on that network…. you can [then] try to get access to credentials that would allow you to manipulate some of the perimeter controls between the corporate network and the control network" – *Industry 3*

Stage 4 – Attack Dynamics:

Scenario 1 – No target response:

"There are some elements in the industry that would know that they're being attacked – emphasize the word 'some'. They wouldn't have a bloody clue. But there are definitely some people in the industry that would know they're under attack… My gut take is most wouldn't have a bloody clue until long after the attackers gone and said 'thanks very much' for whatever they've done." – *Hacker 3*

Scenario 2 – Target response/Counter-response:

"So that would involve isolating the event, bringing, restoring the service up on separate h/w. Once you know that a server's been compromised, you don't even want to shut it down – there could be information in volatile memory spaces that power doesn't lose" – *Industry 1*

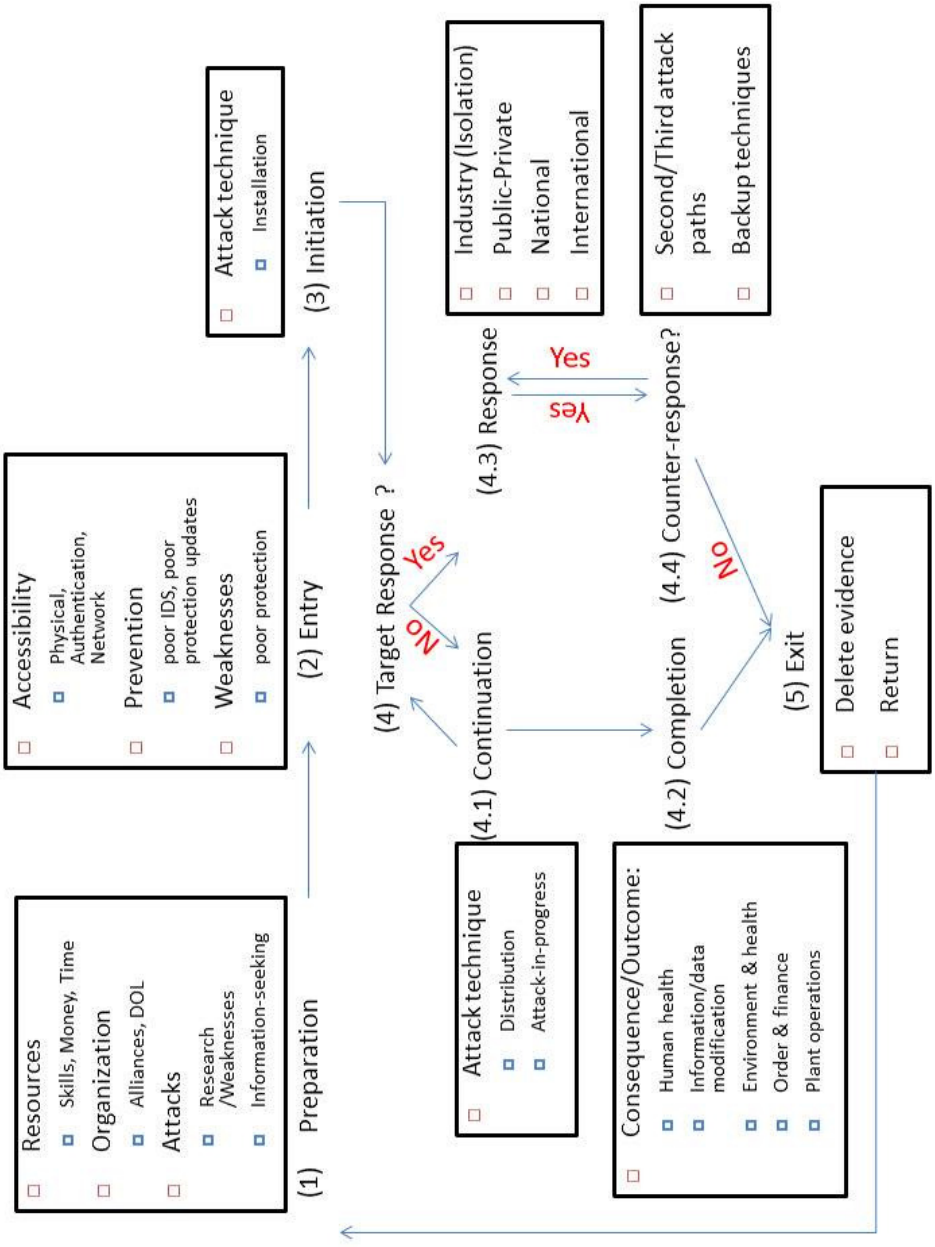
"And so if one of these systems had been isolated I would then try to go through and gain control to one of the other systems." – *Industry 2*

Stage 5 – Exit: "When you get in to the system, you want to try and delete the evidence of what you did to get in, and not leave things in there such that it's easy to detect your presence when you're there or breaking in." – *Hacker 1*

"[if] all my other systems … had been compromised, I would basically go into a hidden mode … and I wouldn't connect to those systems again for another six months to a year until everything's died down and they're no longer paying … attention to what's

happening anymore … I can go back in and start … spreading my control a little bit more" – *Industry 2*

Figure 2: Possible Crime Script



RCT views cybercrime as a goal-oriented choice directed towards accomplishing the criminal's objectives. As such, it is an abstract theory and "requires supplementary empirical content through specification of the relevant aims and choice situations" (Bernasco 2009, p. 6). The dynamic ICS cyberattack process is more appropriately addressed by game theory. Game theory is useful to address the choice situations with which offenders are confronted as they make decisions about target selection, attack technique, strategy modification, attack dynamism, and apprehension evasion.

Game theory is a branch of decision theory concerned with conflict situations (Mit.edu 2001). It is the study of the ways in which *strategic interactions* among *rational players* produce *outcomes* with respect to the *preferences* of those players. A game consists of a set of *players* (at least two), each of which picks a *strategy* (makes a decision) based on information available to him or her (Davis 1983; Martin 1978). Players assess the costs and benefits of each strategy to make informed decisions between several strategies (Mit.edu 2001).

Games can either be sequential or simultaneous. In sequential games, players must alternate moves; in simultaneous games, the players can act at the same time (Mit.edu 2001). These types are distinguished because they require different analytical approaches. Sequential games are those where players have some knowledge about earlier actions; this may not be perfect information about every action of earlier players. Simultaneous games are those where all players make decisions without knowledge of the strategies that are being chosen by other players. Even though decisions may be made at different points in time, the game is simultaneous as each player has no information

about the strategies of others; the game is carried out as if players' decisions were made simultaneously (Gametheory.net 2006).

Game theory provides the language and concepts to capture the constant back and forth 'game' between security/service providers and intruders with respect to cybercrimes against the electricity infrastructure. Cybercriminals are rational players that weigh the pros and cons of each strategy to determine the optimal one with which to target the electricity infrastructure. Targeting the electricity sector's ICS can be viewed as either a sequential or simultaneous game. Sequential games imply that the electricity sector responds to a past successful attack by building a stronger protective measure to prevent further attacks. In response to this new defense tactic, cybercriminals modify their attack strategy to circumvent the latest prevention measure. A simultaneous game involves both the security/service providers and cybercriminals acting concurrently. Here, cybercriminals and the industry are unaware of each other's strategies and therefore an 'outcome' cannot be predicted. Both sequential and simultaneous games are likely to occur in isolation or combination when targeting the electricity sector. For instance, the electricity sector and cybercriminals may not know each other's strategies (simultaneous game), but can later become aware of these, thereby determining their future actions (sequential game).

In particular, game theory extends RCT's decision-making model, by moving from the abstract concept of criminal event to more concrete concepts such as moves, strategies, cooperative and non-cooperative games, and sequential and simultaneous games. While the crime event decision-making model addresses the possibility of unanticipated opposition that may require a change of plan, game theory elaborates on

how these plans are changed via interactive strategies and outcomes, resulting in a continual, adaptive, and evolving game. Integrating game theory, RCT and RAT would require further theoretical evaluation based on scope, coherence, and causality, which should be explored in future research.

Implications for Practice

As noted earlier, this study is based on hacker and industry perceptions, and the implication put forth here are conditional. This study offers six implications for practice that stem from this research, which are summarized in Table 17 below. First, better industry practices are needed on prevention measures, information availability, and system backups. Second, consistent definitions of threat, vulnerability, and consequence should be used throughout the electricity sector. Third, education programs for non-technical industry representatives should be designed. Fourth, mandatory security budgets and testing should be offered. Fifth, there is a need for better regulation and stronger sanctions. Finally, there should be greater collaboration among technical and criminological disciplines.

Table 17: Implications for Practice

Areas	Details
Better Industry Practices	1. Malware-oriented prevention programs 2. Improve real-time intrusion detection 3. Improve authentication practices 4. Limit/isolate internet/email access 5. Limit online ICS information availability 6. Improve system redundancy and backups 7. Engage in frequent, high-quality vulnerability assessments
Definition Consistency	1. Use consistent definition of Threats, Vulnerabilities, and Consequences (TVC) uniformly
Education Programs	1. Educate non-technical industry experts about TVCs
Mandatory Security Budgets	1. Improve industry security testing and vulnerability assessment quality and frequency 2. Improve ICS vendor testing quality and frequency
Improved Regulations & Sanctions	1. Introduce *single* power grid security regulation body 2. Stronger sanctions (temporary suspension of plant operations)
Increased Collaboration	1. Information sharing on ICS vulnerabilities and cyberattack incidents 2. Collaboration between technical and criminological domains

Better Security Practices

This research indicates that the industry should have better security practices in *seven* areas:

1. Malware is the perceived as the most likely technique used in ICS cyberattacks. The industry may therefore want to invest more in malware-oriented prevention measures. Offenders may have to apply greater effort in applying other techniques and therefore be discouraged to engage in ICS cyberattack.
2. Intrusion detection systems (IDS) may not be the most effective measure to detect malicious activity. Human resources to monitor IDS and review entry/exit logs are minimal; improving real-time detection mechanisms is a must.

3. Poor authentication practices permit cybercriminals to easily access ICS. Better password practices, such as encrypting passwords stored or transferred through internal networks, using complex passwords, frequently changing passwords, and not sharing passwords can help curb cybercriminal access to ICS.
4. Ready internet and email access can be exploited by cybercriminals. Thus, providing better connectivity and communication-centric protocols, such as limited internet/email access or separating communication from plant operations, can also provide cybercriminals with fewer avenues of entry.
5. ICS information is easily available through various means, which cybercriminals share at online hacking forums and use to design their attacks. While the industry cannot control the use of hacking forums or attack techniques, it can regulate the amount of ICS information (blueprints, passwords, system versions, and vulnerabilities) available online. By controlling this sensitive information, cybercriminals may find it harder to study their target and design the most appropriate attack, thereby making it harder for them to target ICS.
6. Cybercriminals' desired consequences of electricity ICS cyberattacks are information corruption, inaccurate information processing, and denial/disruption of service. Developing/improving back up databases, information processing systems, and multiple redundant systems to ensure continued operations can be beneficial. Doing so not only ensures system uptime and customer satisfaction, but also deters potential cybercriminals. If their end goal cannot be accomplished, it may deter them from wasting their time and resources in planning, designing, and executing the attack, which decreases the vulnerability of ICS.

7. Industry should also engage in high-quality security and vulnerability assessments on a regular basis. This practice helps identify vulnerabilities that can be addressed before they are exploited. Furthermore, ICS vendors should also engage in better testing before their products are used by industry. [See 'Mandatory Security Budgets' section below]

Definition Consistency

This research identifies several reasons for why industry and hackers have different perceptions of threats, vulnerabilities, and consequences (TVCs). Industry and hackers feel that there is a lack of consensus regarding how TVCs are defined. Furthermore, both hackers and industry believe that *within* their own communities there is no consensus on these terms. The different definitions of these terms is obviously problematic because if there is no clear understanding about these terms, and how they are connected, identifying security issues and risks are not only be flawed, but also vary based on different definitions. These (multiple) incorrect views on TVCs lead to ineffective prevention and security measures. One means of reducing inconsistencies in definitions is through developing a *concise* set of TVCs definitions that are *uniformly* used and practiced *throughout* the industry. This minimizes confusion over definitions, allows common context to compare cyberattack incidents, and helps design effective vulnerability assessments, security testing protocols, and prevention strategies.

Education Programs

Both hackers and industry believe that possessing different knowledge bases affects ICS cybersecurity. Industry members who are not involved in security issues and/or penetration testing activities may possess minimal or no technical expertise to comprehend the importance of vulnerabilities assessments and security testing. Building the knowledge bases of non-technical industry members can be done through education programs. These programs should educate company executives and management on the basic ideas of TVCs, how they are related, and why they are important.

Mandatory Security Budgets & Programs

Both electric utilities and ICS vendors should introduce mandatory security budgets. Each utility should be required to set aside fixed funds solely dedicated to continuous security monitoring, frequent and rigorous security testing, vulnerability assessments, and audits. This mitigates the tensions between industry goals (business and making money) and hacker goals (better security). Vendors should also be required to follow suit. As the analysis demonstrates both hackers and industry agree that only a handful of ICS vendors engage in (poorly developed) testing practices, which undermines their effectiveness. Furthermore, vendors need to continue supporting their products even after industry updates security measures on their end. If the vendor software development cycle is indeed a slow process, energy companies should not have to choose between security and support; rather these security practices and vendor support should be practiced synchronously.

Improved Regulation & Sanctions

Currently, there is no single agency responsible for security regulation for the entire US national grid (Fogarty 2011). Both physical and cyber security responsibilities are split between the North American Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST). Furthermore the regulations set forward by both NERC and NIST are not "strict enough to balance the level of actual threat, and may not any time soon" (Fogarty 2011, p. 2). Current security rules are not enough to hold multi-faceted spear (targeted) phishing attacks and malware-based attacks, which are referred to as "Advanced Persistent Threats" by government security agencies (Fogarty 2011). NIST is pushing for the creation of 'best practices' industry regulations, rather than rules based on actual risks and data countering them (Fogarty 2011). These regulations have received support from the Electric Power Research Institute (EPRI), which is a consortium of utilities and their industries. However, these regulations and the regulating agencies need to have the power and authority to act on these regulations and impose stricter and harsher sanctions. The imposition of fines, for instance, may not be an effective sanction as energy companies may simply view these as the 'cost of doing business'. Sanctions such as temporary suspension of operations till regulatory compliance is achieved may prove more effective in improving security measures.

Increased Collaboration

In November 2011, NERC organized 75 utilities and government agencies into a cybersecurity exercise called GridEx 2011 to test, validate, and adjust existing crisis response plans (Fogarty 2011). GridEx was first effort cross-collaborative effort

undertaken to raise security consciousness in the electricity sector (Fogarty 2011). Such information sharing consortiums are critical because they offer a multi-perspective take on TVCs and bring different knowledge bases together for a more thorough understanding of ICS security. Increasing the diversity of such consortiums, by including psychologists, criminologists, and sociologists can further enhance the quality of such collaborative efforts by addressing the human component of criminal activity. Examining offender decision-making and crime scripts can contribute to the development of an offender-technique-risk matrix which, in turn, can aid in proactively profiling threats and identifying appropriate security measures and effective responses to cyberattacks.

Future Research Studies

This research is exploratory in nature and therefore limited in its scope and generalizability. As such, it offers seven new lines of inquiry for further research, which are summarized in Table 18 below. These research areas include: using alternate research designs; using simulation studies; investigating offender decision-making factors; using game theory to analyze crime scripts; examining the physical aspects of ICS cyberattacks; applying situational crime prevention practices; and extending this research to other critical infrastructures.

Table 18: Future Research

Areas	Details
Primary Data Collection	1. Access apprehended cybercriminals 2. Vignettes 3. Focus Groups
Simulation Studies	1. Simulating ICS environments 2. Simulating offender decision-making using Agent Based Modeling
Offender Decision-making Factors	1. Other factors 2. Factors and Resource Availability 3. Temporal/sequential Nature of Factors 4. Interactive/causal Nature of Factors 5. Risk prediction
Game Theory & Crime Scripts	1. Dynamic Nature of Cybercrime 2. Multiple, overlapping crime scripts
Physical Aspects of ICS Cyberattacks	1. Social engineering 2. Physical access
Situational Crime Prevention	1. Increase Efforts 2. Increase Risks 3. Reduce Rewards 4. Remove Excuses 5. Reduce Provocations
Other Critical Infrastructures	1. PARE RISKS application 2. Crime Scripts

Primary Data Collection

Future research should use alternate methods given the methodological limitations of this study. First, this research did not have access to active offenders and therefore used ethical hackers. It would still be problematic to access cybercriminals actively involved in attacking critical infrastructures because of their underground nature and jurisdictional issues. Accessing apprehended cybercriminals is easier; this choice, however, would also have its own set of limitations. As identified earlier the main types of offenders in electricity sector cyberattacks were individuals who wanted free electricity, organized crime groups who held power grids hostage for extortion money,

and terrorist groups who wanted to damage the power sector and cause fear and panic. The first type of cybercriminal may be easier to access as they are more likely to be in the same geographic boundary as the target. Organized crime groups and terrorist groups may be national or international. If national in jurisdiction, apprehending key and/or technically-savvy members may be difficult. Accessing international groups would be further problematic as they may not be apprehended (nation-sponsored), and if they are apprehended, they may not be accessible to US researchers.

A second method that could prove effective is the use of vignettes that detailed several hypothetical critical infrastructure ICS cyberattacks. These cases can be designed using both industry and hacker input, which may result in cases that are as realistic as possible. Multiple cases can be designed using different combinations of offenders, alliances, resources, and techniques. These cases can then be disseminated at hacking conferences such as DefCon, BlackHat, and Schmoocon, as well as critical infrastructure conferences sponsored by SANS (System Administration and Network Security) and DHS (Department of Homeland Security). Both industry and ethical hackers can respond to these cases, which may offer a common context to compare their responses.

Third, mixed focus groups of hackers and industry can also be conducted using the same vignettes, which may generate a rich and insightful discussion on ICS TVCs. Focus groups can be more useful than one-on-one interviews as the comments made by each participant are available to other participants, which can initiate dialog, stimulate alternate interpretations, and offer more in-depth information resulting from greater response clarity in group discussions. Regardless of the methodological means used to

study ICS cybercrimes, future studies can address the ten research questions identified in this research. These findings which can be triangulated with those that emerged here.

Simulation Studies

As noted earlier, access to 'real-time' data or observing an ICS cybercrime unfold is problematic, which can be useful in understanding the crime process. Points of entry, attack progression, and conclusion can shed light on offender decision-making processes at each stage of the crime process. While accessing a cybercrime in progress, especially against critical infrastructures is very difficult for national security and sensitivity reasons, infrastructure attack simulations can be conducted. Simulation studies have been conducted, but their results are not publicly available. Simulations can be conducted using computer-based programs that replicate ICS environments, as well as their vulnerabilities, prevention measures, and accessibility issues.

Simulation studies can be supplemented by using agent-based-modeling (ABM) systems, which are modeled as a collection of autonomous decision-making entities (agents). Each agent can individually assess its situation and can make decisions on the basis of a set of rules. These rules can be obtained from penetration testers who are recruited to 'break into' ICS. Thus, they possess the same set of decision-making abilities as malicious agents. This interaction between simulated environments and agents can be extremely useful in studying multiple ICS cyberattacks. By altering any single element (vulnerabilities, prevention measures, access points, agent decision rules), a rigorous analysis of numerous crime processes can be obtained.

Factors Influencing Offender Decision-Making

Future research should further delve into factors influencing offender decision-making. The factors identified in this research serve as a starting point and need to be examined in greater depth. First, each of the three methods identified above could be used to also identify any new factors as well as whether the factors from this research are relevant. Second, it is very likely that the factors influencing offender decision-making vary according to the different organizations, goals, and skills. For instance, organized crime groups may have different sets of resources than state-sponsored crime groups, which would in turn affect each stage of the crime script.

Third, this research only offered a preliminary analysis of the temporal or sequential nature of the PARE RISKS factors. Factors may also have a multiple or overlapping presence in the crime script. For instance, research and development may happen at the preparation stage, and again during the counter response stage when cybercriminals may need to research alternate techniques or entry points to continue the attack.

A fourth area of interest would be to determine if the PARE RISKS factors are interactive and/or causal. For instance (how) does the interaction between the monetary and temporal resources influence other factors in the same stage (preparation), such as the choice of attack techniques, or other stages, such as countering an industry response? Would cybercriminals have enough time and money to continue with the attack? These are also important issues to address as they directly impact offender decision-making and ICS security.

Finally, if a comprehensive and (near) exhaustive set of factors can be determined, they can be mapped into larger categories of threats (T), vulnerabilities (V), and consequences (C), which could be used, in turn, to determine risk. Risk can be viewed as a function of TVC: R = *f* (T,V,C). Identifying TVC factors could also be useful in conducting inferential statistics. For instance, logistic regression could be conducted to determine whether or not potential offenders would target ICS. Multiple regression could also be conducted to determine a risk equation based on threat, vulnerability, and consequence predictors.

Game Theory & Crime Scripts

Developing game theory in the context of critical infrastructure cyberattacks is another area of future research. This research identified three possible means of countering cyberattacks: isolation; reconnaissance; and misleading the enemy. This research only offered insights into the counter-response for isolation, via alternate access and techniques. The details of how these alternate access and techniques play out remain unclear. Furthermore, how cybercriminals would respond to reconnaissance and false feedback is also unknown. Game theory could be used to guide possible 'play' scenarios between industry and cybercriminals. Furthermore, game theory could be applied via agent-based modeling (ABM). Both industry and cybercriminal agents could be created with a set of decision rules to determine how the cybercrime game would unfold. This strategy would make a great contribution to understanding offender decision-making factors and the effectiveness of prevention measures and industry response.

This research offered one possible, rather rudimentary, crime script for critical infrastructure cyberattacks. It is very likely, however, that crime scripts are complex. For instance the crime script identified in this research could very well be comprised of smaller, multiple, and interactive crime scripts. For instance, the entry stage itself could have several crime scripts for how to enter the system, thwart prevention measures, and exploit system weaknesses. This research identified five stages of the crime script, and each could have several other crime scripts embedded in it. Future studies should examine this intricate and multitudinous nature of crime scripts. Furthermore, crime scripts may be simultaneous and/or sequential. Some crime scripts may need to be completed before others can begin. For example, crime scripts for entering the system will need to occur before crime scripts for the actual attack can commence. Alternatively, multiple crime scripts may need to occur simultaneously. For instance, crime scripts for accessibility, prevention measures, and exploiting weaknesses may all need to occur at the same time to enter the targeted system. This temporal nature of crime scripts would also therefore be another useful area of research to understand offender decision-making.

Physical Components of ICS Cyberattacks

The interviews suggested that critical infrastructure cyberattacks had a physical component to them. First, social engineering was a very important technique used in researching and executing cyberattacks against critical infrastructures. Social engineering was a strategy used to trick individuals into divulging sensitive information by obtaining their trust. These techniques could be both physical and digital in form. Second, digital attacks could also be combined with physical attacks (tampering with physical devices)

against critical infrastructures. In some cases, physical techniques were used to initiate cyber techniques. For instance, obtaining physical access to a corporate office was essential to install malware programs onto company computers. Thus, understanding the physical-cyber relationship could also serve as a useful research area.

Situational Crime Prevention

This research focused on the decision-making processes of offenders based on their digital environments; it examined factors that made a target suitable based on its accessibility, prevention measures, system weaknesses, and ability to respond to cyberattacks. Understanding what makes the target suitable is essential in developing strategies that make it 'unattractive'. Situational crime prevention (SCP), which is primarily a crime prevention measure, focuses on reducing crime opportunities rather than on the characteristics of offenders. It emphasizes that crime and criminality is often determined by the existence of an attractive opportunity to commit crimes. As such, SCP offers 25 techniques of crime prevention based on five principal categories of action: (i) increasing the effort required by the offender to commit the crime by hardening targets, controlling access to facilities, screening entry and exit points, deflecting offenders, and controlling attack tools, (ii) increasing the risks of detection by extending guardianship, improving surveillance, reducing anonymity, and using real-time, continuous monitoring systems, (iii) reducing the rewards of critical infrastructures attacks by removing the online presence or links to ICS, disrupting virtual black markets where exploits are traded, (iv) removing excuses by educating employees, reducing temptations of insider crimes, reducing frustrations and stress in ICS environments, and (v) reducing

provocations by setting formal regulatory policies, posting instructions on incident-response protocols, and assisting with security and vulnerability compliance guidelines (Clarke 2008). Future research could therefore apply SCP principles to electricity ICS cyberattacks to reduce crime opportunities.

Other Critical Infrastructures

While this research examined cyberattacks against the electricity sector, several other critical infrastructures, such as water, transportation, and finance, are also subjected to cyberattacks. Another area of research is to determine the degree to which factors influencing offender decision-making vary across multiple infrastructures. Issues of factor sequence, interaction, and causality addressed above can be considered. Similarly, the crime processes for other infrastructures, and their multiple, interactive, and temporal aspects can also be compared. Finally, research can also examine whether different infrastructures experience different types of attacks (frequency, duration, intensity) from different threat agents (terrorists, organized crime groups, nation states, individuals). This would improve our understanding of critical infrastructure attacks and offender decision-making, help develop and offender-technique profile matrix, and offer insight into the effective application of situational crime prevention principles.

Conclusion

This research compared the views of ethical hackers and industry experts on electricity sector threats, vulnerabilities, and consequences (TVCs), as well as offender decision-making. It identified nine rudimentary factors that influenced decision-making which were summarized via the PARE RISKS framework: Prevention measures; Attacks

and Alliances; Result; Ease of Access; Response and Recovery; Interconnectedness and Interdependencies; Security Testing, Assessments, and Audits; Knowledge, Skills, Research and Development; and System Weaknesses. This framework was modified slightly to capture the industry and hacker perception analysis. It also generated a preliminary electricity ICS cybercrime script identifying which factors were relevant at different stages in the crime process.

Four important findings emerged from this study. First, hackers and industry had minimal differences in how they viewed ICS TVCs. Hackers were more likely than industry respondents to believe that cybercriminals engaged in target research, exploited internet and email access, as well as poor password practices. Industry respondents were, not surprisingly, more concerned with the outcomes of ICS cyberattacks. Second, the PARE RISKS framework is a rudimentary set of factors that influence offender decision-making. These factors, however, are very likely to be more complex, dynamic, interactive, and sequential in nature. Third, ICS cybercrimes extend beyond the actual crime; these crimes are processes, complete with sophisticated crime scripts. Finally, ICS cybercrimes are *not* exclusively cyber, they have important physical aspects to them. As such, these crimes should not be viewed through an exclusively cyber lens; research should acknowledge the hybridity of these crimes.

While this exploratory research relied on industry and hacker perceptions, it revealed important findings that moved beyond technical ICS security and vulnerability assessments. This study offered a preliminary means of obtaining a more well-rounded understanding of electricity sector ICS cyberattacks. Though small-scale in scope, this research actively engaged hackers and industry experts in a dialogue about critical

infrastructure cyberattacks. Communication between academics, industry, and hackers was (and will continue to be) crucial in obtaining a better understanding of ICS TVCs and offender decision-making. This dissertation serves as a point of departure for future studies; researchers can use the factors and initial crime script identified here as a foundation for more in-depth studies. Additionally, the seven areas developed for future studies could also be pursued by academics in partnership with the hacking and industry communities. Hopefully, this research will stimulate new ways of conceptualizing offender decision-making and crime processes, ultimately contributing further to the fields of criminology and critical infrastructure studies.

References

Amin, M. (2004). *North American Electricity Infrastructure: System Security, Quality, Reliability, Availability, and Efficiency Challenges and their Societal Impacts*. Retrieved February 16, 2010. Online at http://160.94.126.215/amin/nsf_chapter2.pdf.

Archibugi, D. & Pietrobelli, C. (2003). The Globalisation of Technology and Its Implications for Developing Countries: Windows of Opportunity or Further Burden? *Technological Forecasting and Social Change, 70*(9), 861-883.

Barber, B. (1995). *Jihad vs. McWorld*. New York: Random House.

BBC (British Broadcasting Corporation). (2011). *US and Israel were behind Stuxnet claims researcher*. Retrieved August 17, 2011. Online at http://www.bbc.co.uk/news/technology-12633240

Bednarski, G. (2004). *Enumerating and Reducing the Threat of Transnational Cyber Extortion against Small and Medium Size Organizations*. Retrieved September 13, 2005, from Carnegie Mellon University. Online at http://www.andrew.cmu.edu/user/gbednars/InformationWeek CMU_Cyber_Extortion_Study.pdf

Bernasco, W. (2009). Foraging Strategies of Homo Criminals: Lessons from Behavioral Ecology. *Crime Patterns and Analysis, 2* (1), pp. 5-16.

Bertram, D. (2007). *Likert Scales… are the meaning of life*. Retrieved October 2, 2011. Online at http://pages.cpsc.ucalgary.ca/~saul/wiki/uploads/CPSC681/topic-dane-likert.pdf

Blane, J.V. (2002). *Cyberwarfare: Terror at a Click*. NY: Novinka Books.

Block, D. (2004). Globalization, Transnational Communication and the Internet. *IJMS: International Journal on Multicultural Societies, 6*(1), 22-37.

BMJ.com (1997). *Measurement error and bias*. Retrieved April 18, 2009. Online at http://www.bmj.com/epidem/epid.4.html

Broad, W., Markoff, J. & Sanger, D. (2011). *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. Retrieved August 17, 2011. Online at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Byres, E.J. & Lowe, J. (2004). The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, VDE 2004 Congress, VDE, Berlin, October 2004.

Carr, E. & Worth, A. (2001). The Use of the Telephone Interview for Research. *Nursing Times Research, 6*(1), 511-524.

Cary, A. (2011). *PNNL still recovering from cyberattack*. Retrieved August 17, 2011. Online at http://www.tri-cityherald.com/2011/07/09/1560790/pnnl-still-recovering-from-cyberattack.html

Clarke, R. (2008). Situational Crime Prevention. In R. Wortley & L. Mazerolle. (Eds.), *Environmental Criminology and Crime Analysis* (pp. 178-194). Oregon: Willan Publishing.

Clarke, R. & Felson, M. (2008). Introduction: Criminology, Routine Activity, and Rational Choice. In R. Clarke & M. Felson. (Eds.), *Advances in Criminological Theory, Volume 5* (pp. 1-14) NJ: Transaction Publishers.

Cohen, L. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*, pp. 588-608.

Cook, C., Heath, F., & Thompson, R. (2000) A meta-analysis of response rates in web or Internet-based surveys. *Educational and Psychological Measurement, 60*(6), 821-836.

Copeland, C. & Cody, B. (2006). *Terrorism and Security Issues Facing the Water Infrastructure Sector*. Congressional Research Service Report for Congress. Retrieved April 4, 2009.
Online at http://www.fas.org/irp/crs/RS21026.pdf

Cornish, D. & Clarke, R. (2008). The Rational Choice Perspective. In R. Wortley & L. Mazerolle. (Eds.), *Environmental Criminology and Crime Analysis* (pp. 21-47). Oregon: Willan Publishing.

Cortina, J.M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78,* pp. 98-104.

Costello, A. & Osborne, J. (2005). Best Practices in Exploratory Factory Analysis: Four Recommendations for Getting the Most From Your Analysis. *Practical Assessment, Research & Evaluation, 10*(7), pp. 1-9.

Datz, T. (2004). *Out of Control*. Retrieved March 8, 2006. Online at http://www.csoonline.com/read/080104/control.html

Davis, M. (1983). *Game Theory: A Nontechnical Introduction*. NY: Dover Publications, Inc.

Decker, (2005). *Using Offender Interviews to Inform Problem Solving*. Problem-Oriented Guides for Police Problem-Solving Tools Series. Guide No. 3. Retrieved April 12, 2009. Online at http://www.popcenter.org/tools/pdfs/InterviewingOffenders.pdf

Denzin, N. (1978a). *The Research Act*. NY: McGraw Hill, 2nd ed.

Denzin, N. (1978b). *Sociological Methods: A Sourcebook*, NY: McGraw Hill, 2nd ed.

DHS (Department of Homeland Security). (2008). *Infrastructure Taxonomy, Version 3: November 1, 2008*. Infrastructure Information Collection Division (IICD). Office of Infrastructure Protection.

DHS (2010). *Risk Steering Committee DHS Risk Lexicon - 2010 Edition. September 2010*. Retrieved August 1, 2011. Online at http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

DHS (2011). Common Cybersecurity Vulnerabilities in Industrial Control Systems. Retrieved January 15, 2012. Online at http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

DPS Telecom (2011a). *SCADA Knowledge Base*. Retrieved August 5, 2011. Online at http://www.dpstele.com/dpsnews/techinfo/scada/scada_knowledge_base.php

DPS Telecom (2011b). *DCS vs. SCADA in Modern Environments*. Retrieved August 9, 2011. Online at http://www.dpstele.com/dpsnews/techinfo/scada/dcs_vs_scada.php

EIA (Energy Information Administration) (2007). *Electric Power Industry Overview 2007*. Retrieved January 30, 2012. Online at http://www.eia.gov/cneaf/electricity/page/prim2/toc2.html

EIA (2009).*What is the electric power grid, and what are some challenges it faces?* Retrieved January 30, 2012. Online at http://www.eia.gov/energy_in_brief/power_grid.cfm

Einstadter, W. & Henry, S. (1995). Criminological Theory: An Analysis of its Underlying Assumptions. Fort Worth, TX: Harcourt, Brace and Company.

EnergySec (2011). *Welcome*. Retrieved December 1, 2011. Online at http://www.energysec.org

Ezell, B. (1998). *Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply*. Retrieved April 2, 2009. Online at http://www.riskinfo.com/cyberisk/Watersupply/SCADA-thesis.html

Falliere, N., Murchu, L. & Chien, E. (2011). *W32.Stuxnet Dossier, Version 1.4*. Retrieved August 18, 2011. Online at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Fabrigar, L. R., Wegener, D. T., MacCallum, D. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods, 4*(3), 272-299.

Ferguson, E. & Cox, T. (1993). Exploratory Factor Analysis: A User's Guide. *International Justice of Selection and Assessment, 1*(2), pp. 84-94.

Field, A. (2005). *Discovering Statistics Using SPSS*. London: Sage Publications, Ltd.

Fogarty, K. (2011). *U.S. power grid is a big, soft target for cyberattack, MIT study shows*. Retrieved December 7, 2011. Online at http://www.itworld.com/print/230469

Gametheory.net (2006). *Simultaneous Games*. Retrieved May 23, 2010. Online at http://www.gametheory.net/Dictionary/SimultaneousGame.html

GAO (General Accounting Office). (2003). *Critical Infrastructure Protection: Challenges in Securing Control Systems*. Retrieved March 20, 2010. Online at http://www.gao.gov/new.items/d04140t.pdf

GAO (2005). *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges*. Retrieved April 6, 2009. Online at http://www.gao.gov/new.items/d05327.pdf

Gorman, S. (2009). *Electricity Grid in U.S. Penetrated by Spies.* http://online.wsj.com/article/SB123914805204099085.html

Gorsuch, R. L. (1989). Common factor analysis versus component analysis: Some well and little known facts. *Multivariate Behavioral Research, 25*, 33-39.

Grant, N. & Fabrigar, L. (2007). Exploratory Factor Analysis. In N. Salkind and K. Rasmussen (Eds.). *Encyclopedia of Measurement and Statistics* (pp. 332-335). CA: Sage Publications, Inc.

Haggerty, K.D. & Ericson, R.V. (2000). The Surveillant Assemblage. *British Journal of Sociology, 51*(4), 605-622.

Haimes, Y. (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. *Risk Analysis, 26*(2), pp. 293-296.

INL (Idaho National Laboratory). (2010). NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses. Retrieved January 15, 2012. Online at http://www.fas.org/sgp/eprint/nstb.pdf

Infracritical.com (2011). *SCADASEC-L Usage Policy*. Retrieved December 1, 2011. Online at http://www.infracritical.com/?page_id=33

Internetworldstats.com (2010). *World Internet Usage Statistics News and World Population Stats*. Retrieved February 9, 2010. Online at http://www.internetworldstats.com/stats.htm

Jackson, W. (2011a). *Cyberattacks take two Energy labs offline*. Retrieved August 10, 2011. Online at http://gcn.com/Articles/2011/07/06/Cyber-attacks-take-2-energy-labs-offline.aspx?s=secur

Jackson, W. (2011b). *Energy lab back online after cyberattack*. Retrieved August 17, 2011. Online at http://fcw.com/articles/2011/07/15/pnnl-back-online-after-hack.aspx

Jaishankar, K. (2009). Space Transition Theory of Cybercrimes. In F. Schmalleger & M. Pittaro. (Eds.). *Crimes of the Internet* (pp. 283-301). New Jersey: Pearson Prentice Hall.

Jewkes, Y. (2003). *Dot.cons: Crime, deviance and identity on the Internet*. Oregon: Willan Publishing.

Jick, T. (1979). Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly, 24* (4), pp. 602-611.

Jones, S.G.(1995).*Cybersociety: Computer-mediated Communication and Community*. Thousand Oaks, CA: Sage.

Kellner, D. (2001). Globalisation, Technopolitics and Revolution. *Theoria (Pietermaritzburg), 98*, 14-34.

King, N. & Horrocks, C. (2010). *Interviews in Qualitative Research*. California: SAGE Publications Inc.

Krone, T. (2005). *Hacking Motives*. Retrieved March 8, 2006. Online at http://www.aic.gov.au/publications/htcb/htcb006.pdf

Kuvshinkova, S. (2003). *SQL SLAMMER worm lessons learned for consideration by the electricity sector*. Retrieved September 21, 2011. Online at http://www.myitforum.com/articles/15/view.asp?id=5985

Lemos, R. (2000). *Power play: Electric company hacked*. Retrieved September 20, 2011. Online at http://www.zdnet.co.uk/news/emerging-tech/2000/12/15/power-play-electric-company-hacked-2083210/

Lonsdale, C., Hodge, K., & Rose, E.A. (2006). Pixels vs. paper: Comparing online and traditional survey methods in sport psychology. *Journal of Sport and Exercise Psychology, 28*, pp. 100–108

Ludlow, P. (1996). *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. Cambridge, Massachusetts: MIT Press.

Luiijf, E. (2008). SCADA Security Good Practices for the Drinking Water Sector. Retrieved April 3, 2009. Online at http://www.tno.nl/content.cfm?context=markten&content=publicatie&laag1=194&laag2=1&item_id=404&Taal=2

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Martin, B. (1978). The Selective Usefulness of Game Theory. *Social Studies of Science, 8*, pp. 85-110.

Mason, J. (2002). *Qualitative Researching - 2nd edition.* London: Sage Publications Inc.

Maxfield, M. & Babbie, E. (2005). *Research Methods For Criminal Justice and Criminology 4th Edition*. Wadsworth Publishing.

McAfee. (2005). *McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet*. Retrieved October 20, 2005. Online at http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf

McMillan, R. (2011). *A Power Plant Hack That Anybody Could Use*. Retrieved August 5, 2011. Online at http://www.pcworld.com/businesscenter/article/237347/a_power_plant_hack_that_anybody_could_use.html

McMullan, J. & Rege, A. (2007). Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges. *Gaming Law Review, 11*(6), 648-665.

Mills, E. (2011). *Researchers warn of SCADA equipment discoverable via Google*. Retrieved August 5, 2011. Online at http://news.cnet.com/8301-27080_3-20087201-245/researchers-warn-of-scada-equipment-discoverable-via-google/

Mit.edu (2001). *Game Theory*. Retrieved February 23, 2010. Online at http://msl1.mit.edu/ESD10/block4/4.4_-_Game_Theory.pdf.

Morain, D. (2001). *Hackers Victimize Cal-ISO*. Retrieved August 18, 2011. Online at http://articles.latimes.com/2001/jun/09/news/mn-8294

Moteff, J. (2005). *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Retrieved August 1, 2011. Online at http://www.fas.org/sgp/crs/homesec/RL32561.pdf

NERC (North American Electric Reliability Corporation) (2010). *NERC: About NERC.* Retrieved March 19, 2010. Online at http://www.nerc.com/page.php?cid=1

Neuman, L. W. (2003). *Social Research Methods: Qualitative and Quantitative Approaches*. Massachusetts: Allyn & Bacon.

Newman, G. & Clarke, R. (2003). Superhighway Robbery: Preventing e-commerce crime. Oregon: Willan Publishing.

Newsom, J. (2005). *A Quick Primer on Exploratory Factor Analysis*. Retrieved October 21, 2011. Online at www.upa.pdx.edu/IOA/newsom/semclass/ho_efa.doc

Nicholson, R. (2008). *Critical Infrastructure Cybersecurity: Survey Findings and Analysis*. Energy Insights, November 2008.

NSTAC (National Security Telecommunications Advisory Committee) (2000). *Information Assurance Task Force: Electric Power Risk Assessment – Executive Summary*. Retrieved August 17, 2011. Online at http://www.solarstorms.org/ElectricAssessment.html

O'Donoghue, T., Punch K. (2003). *Qualitative Educational Research in Action: Doing and Reflecting*. London: Routledge.

Oldenburg, R. (1989). *The Great Good Place: Cafes, Coffee Shops, Community Centers, Beauty Parlors, General Stores, Bars, Hangouts, and How They Get You Through the Day*. New York: Paragon House.

Oman, P., Schweitzer III, E. and Robert, J. (2001). *Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions*. Schweitzer Engineering Laboratories. Retrieved August 11, 2011. Online at http://www.selinc.com/techpprs/6118.pdf

Pedhazur, E. J., & Schmelkin, L. P. (1991). *Measurement, design, and analysis: An integrated approach.* Hillsdale, NJ: Erlbaum.

Poster, M. (1995). Databases as Discourse, or Electronic Interpellations, in *The Second Media Age*. Polity Press.

Poulsen, K. (2003). *Slammer worm crashed Ohio nuke plant network*. Retrieved August 10, 2011. Online at http://www.securityfocus.com/news/6767

Public Citizen (2004). *Water Unsecured: Public Drinking Water is Vulnerable to Terrorist Attack*. Retrieved April 3, 2009. Online at http://www.citizen.org/documents/Water.pdf

PureVPN (2011). *A Sophisticated Cyber Attack Forces DOE to Shut Down*. Retrieved August 17, 2011. Online at http://www.purevpn.com/blog/cyber-attack-forces-doe-to-shut-down/

QSR International (2011a). *What is Qualitative Research?* Retrieved December 19, 2011. Online at http://www.qsrinternational.com/what-is-qualitative-research.aspx

QSR International (2011b). *NVivo 9 – Features and Benefits* Retrieved December 19, 2011. Online at http://www.qsrinternational.com/products_nvivo_features-and-benefits.aspx

Rantala, R. (2008). *Cybercrimes Against Businesses, 2005*. Bureau of Justice Statistics. Retrieved February 19, 2009, from http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf

Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology, 3* (2), pp. 494-513.

Rege-Patwardhan, A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies, 22* (3).

Reid,E. (1994) *Cultural formations in Text Based Virtual reality*. Retrieved June 23, 2007. Online at http://www.ludd.luth.se/mud/aber/articles/cult-form.thesis.html

Reuters. (2006). *Israel holds couple in corporate espionage case*. Retrieved March 8, 2006. Online at http://news.zdnet.com/2100-1009_22-6033129.html
Rheingold, H. (1993). *The Virtual Community: Homesteading on the Electronic Frontier*. MA: Addison-Wesley.

Ritzer, G. (1996). *The McDonaldization of Society*. London: Sage.

Robles, R., Choi, M., Cho, E., Kim, S., Park, G. & Lee, J. (2008). Common Threats and Vulnerabilities of Critical Infrastructures. *International Journal of Control and Automation, 1*(1), pp. 17-22.

Rogers, M.K. (2005). *The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach*. Retrieved January 23, 2007. Online at https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-43.pdf

Rossignol, M. (2001). *Critical Infrastructure Protection and Emergency Preparedness*. Retrieved August 27, 2007, from http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/BP/prb017-e.htm

SANS (System Administration, Networking, and Security Institute) (2011a). *Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack*. Retrieved August 30, 2011. Online at http://www.sans.org/reading_room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack_606

SANS (2011b). *About the SANS Institute*. Retrieved December 1, 2011. Online at http://www.sans.org/about/sans.php.

Scadasystems.net (2011). *SCADA systems*. Retrieved August 9, 2011. Online at http://www.scadasystems.net/

Shadish, W., Cook, T., & Campbell, D. (2002). *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Houghton Mifflin Company.

Shoemaker, P., Tankard Jr., J., Lasorsa, D. (2004). *How to Build Social Science Theories*. California: Sage Publications, Inc.

Siddiqui, D. (1998). Information Technologies and Globalization: Ruination vs. Ripples. *The American Journal of Islamic Social Sciences, 15*(3), 45-79.

Smith, R., Grabosky, P. & Urbas, G. (2004). *Cybercriminals on Trial*. New York: Cambridge University Press.

Stamp, J., Dillinger, J., Young, W. & DePoy, J. (2003). *Common Vulnerabilities in Critical Infrastructure Control Systems*. Retrieved August 27, 2007, from http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf

Staples, W.G. (2000). *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Maryland: Rowman & Littlefield Publishers, Inc.

Stevens, J. (1992). *Applied Multivariate Statistics for the Social Science – 2nd ed*. NJ: Erlbaum, Hillsdale.

Stouffer, K., Falco, J. & Scarfone, K. (2011). *NIST Guide to Industrial Control Systems (ICS) Security*. Retrieved August 5, 2011. Online at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Surveysystem.com (2009). Survey Design. Retrieved April 17, 2009. Online at http://www.surveysystem.com/sdesign.htm

Swenson, D. (1999). *How to Evaluate a Theory*. Retrieved April 25, 2008. Online at http://faculty.css.edu/dswenson/web/theoryeval.html

Symantec (2007).*What is Cybercrime?* Retrieved July 3, 2007, from http://www.symantec.com/avcenter/cybercrime/index_page2.html

Tabachnick, B. G., & Fidell, L. S. (2007). *Using Multivariate Statistics, 5th ed*. MA: Allyn and Bacon.

Taylor, R.W., Caeti, T.J., Loper, D.K., Fritsch, E.J., & Liederbach, J. (2006). *Digital Crime and Digital Terrorism*. NJ: Pearson Education, Inc.

Tourangeau, R. (2004). Survey Research and Societal Change. *Annual Review Psychology, 55*, 227-801.

Turkle, S. (1997). Multiple Subjectivity and Virtual Community at the End of the Freudian Century. *Sociological Inquiry, 67* (1), 72-83.

Verton, D. (2003). *Black Ice: The Invisible Threat of Cyber-Terrorism*. CA: McGraw-Hill.

Wagner, D. (1984). *The Growth of Sociological Theories*. California: Sage Publications, Inc.

Warner, B. (2001). *Hackers Heaven: Online Gambling*. Retrieved September 14, 2005, from CBS News. Online at http://www.cbsnews.com/stories/2001/09/10/tech/main310567.shtml

Weaver, N., Paxson, V., Staniford, S. & Cunningham, R. (2003). *A Taxonomy of Computer Worms*. University of Berkley. Retrieved March 8, 2006. Online at http://www.cs.berkeley.edu/~nweaver/papers/taxonomy.pdf

Whitaker, R. (1999). The End of Privacy: How Total Surveillance is Becoming a Reality. New York: The New Press.

WSCCCSWG (Water Sector Coordinating Council Cyber Security Working Group) (2008). *Roadmap to Secure Control Systems in the Water Sector*. Retrieved April 4, 2009. Online at http://www.nawc.org/pdf/Final%20Water%20Security%20Roadmap%2003-19-08.pdf

Yar (2006). *Cybercrime and Society*. California: Sage Publications Ltd.

Yin, Robert K. (2008) *Case study research: design and methods*, 4th edition, Thousand Oaks, CA: Sage Publications.

YouTube (2009). *SCADA Tutorial*. Retrieved August 5, 2011. Online at http://www.youtube.com/watch?v=tIU_wDVoEVE

ZDNN (2001). *Humans opened the door for power hack*. Retrieved August 18, 2011. Online at http://www.zdnet.com/news/humans-opened-the-door-for-calif-power-hack/117607

Zintro (2011). *SCADA Experts - Find SCADA Consultants, Expert Witnesses & More* Retrieved August 5, 2011. https://www.zintro.com/area/scada

Appendix A: Survey Instrument

Section One (Administrative):

1. Are you representing the electricity industry or the hacker group (Circle one)? Hacker/Industry
2. Do you expect to see a difference between hacker and industry perceptions regarding ICS cybervulnerabilities (Circle one)? Difference/No Difference
3. How familiar are you with ICS systems in general? Please rank 1-5 where 1 is the lowest familiarity and 5 is the highest: 1 2 3 4 5
4. How familiar are you with ICS systems used in the electricity sector? Please rank 1-5 where 1 is the lowest familiarity and 5 is the highest: 1 2 3 4 5

For sections two to ten, please state *your opinion on how **cybercriminals may think, target, and attack ICS***.

Section Two (Accessibility):

1. How often do cybercriminals target the electricity sector's ICS systems in a one-year period (Circle one)?
   1-10 11-20 21-30 31-40 >41
2. Please rank which frequency of remote access used by facility operators is ideal for a successful attack (Circle one)?
   <10 hrs/wk 10-20 hrs/wk 21-30 hrs/wk 31-40 hrs/wk > 40 hrs/wk
3. Can cybercriminals exploit internet access for facility operators even if it is restricted? Yes/No
4. Can cybercriminals exploit email access for facility operators even if it is restricted? Yes/No
5. What minimum connection speed do cybercriminals need to conduct an attack (Circle one)?
   <1 kbps 1-50 kbps 51-100 kbps 101-150 kbps > 150 kbps
6. Which remote access approach would be beneficial to cybercriminals (Rank 1-5 where 1 is the least ideal and 5 is the most ideal)?
   Dial-up connection 1 2 3 4 5 Intranet 1 2 3 4 5
   Wide Area Network 1 2 3 4 5 Virtual Private Network 1 2 3 4 5

Section Three (Countermeasures):

1. Which frequency of firewall updates would make an ICS cyberattack more likely (Circle all that apply and then rank 1-5 where 1 is the least likely and 5 is the most likely)?

Daily 1 2 3 4 5	Weekly 1 2 3 4 5	Monthly 1 2 3 4 5	Quarterly 1 2 3 4 5
Semi-annually 1 2 3 4 5	Annually 1 2 3 4 5	< 1/yr 1 2 3 4 5	Never 1 2 3 4 5

2. Which frequency of antivirus software updates would make an ICS cyberattack more likely (Circle all that apply and then rank 1-5 where 1 is the least likely and 5 is the most likely)?

Daily 1 2 3 4 5	Weekly 1 2 3 4 5	Monthly 1 2 3 4 5	Quarterly 1 2 3 4 5
Semi-annually 1 2 3 4 5	Annually 1 2 3 4 5	< 1/year 1 2 3 4 5	Never 1 2 3 4 5

3. Which frequency of security patch updates would make an ICS cyberattack more likely (Circle all that apply and then rank 1-5 where 1 is the least likely and 5 is the most likely)?

Daily 1 2 3 4 5	Weekly 1 2 3 4 5	Monthly 1 2 3 4 5	Quarterly 1 2 3 4 5
Semi-annually 1 2 3 4 5	Annually 1 2 3 4 5	< 1/year 1 2 3 4 5	Never 1 2 3 4 5

4. How easy is it to bypass intrusion detection systems (IDS) to access the electricity plant? Please rank 1-5 where 1 is easy and 5 is difficult: 1 2 3 4 5

5. Which IDS is easier to bypass (Circle all that apply and then rank 1 for easiest to bypass and 5 for the most difficult)?

Perimeter access logging	1 2 3 4 5
Network detection system	1 2 3 4 5
Host IDS (tripwire, fileagent)	1 2 3 4 5

6. How much time would cybercriminals spend countering security measures before giving up on the target (Circle one)?

< 1 hr 1 day few days 1 wk > 1 wk

Section Four (System Weaknesses):

1. Do cybercriminals believe the design, configuration, and implementation of ICS systems used by electricity sectors is safe from unauthorized access? Yes/No

2. Do cybercriminals believe the design, configuration, and implementation of ICS systems used by electricity sectors is safe from unauthorized use? Yes/No

3. Which ICS *Platform* vulnerability results in a successful attack [Appendix A: ICS Vulnerabilities]? Please rank 1-5 where 1 is the least successful and 5 is the most:
    a. Configuration vulnerability
        i. OS and security patches are not maintained 1 2 3 4 5
        ii. OS and security patches are implemented without thorough testing 1 2 3 4 5
        iii. Poor password practices (no password used, password disclosure) 1 2 3 4 5
        iv. Operating System (OS) and security patches are not developed until significantly after security vulnerabilities are found 1 2 3 4 5
    b. Hardware (h/w) vulnerability
        i. Lack of backup power 1 2 3 4 5
        ii. Lack of redundancy for critical components 1 2 3 4 5
        iii. Insecure remote access on ICS components 1 2 3 4 5
        iv. Unauthorized personnel have physical access to equipment 1 2 3 4 5
    c. Software (s/w) vulnerability
        i. Buffer overflow 1 2 3 4 5
        ii. Poor or nonexistent virus protection 1 2 3 4 5
        iii. Poor or nonexistent file integrity checking 1 2 3 4 5
        iv. Poor or nonexistent denial of service (DoS) protection 1 2 3 4 5
        v. Inadequate authentication and access control for software 1 2 3 4 5
        vi. Intrusion detection/prevention software not installed/maintained 1 2 3 4 5
        vii. Use of proprietary software that has been discussed at conferences and in periodicals 1 2 3 4 5

4. Which ICS *Network* vulnerability results in a successful attack [Appendix A: ICS Vulnerabilities]? Please rank 1-5 where 1 is the least successful and 5 is the most:
    a. Configuration vulnerability
        i. Passwords not encrypted in transit 1 2 3 4 5
        ii. Inadequate access controls applied 1 2 3 4 5
        iii. Weak network security architecture 1 2 3 4 5
        iv. Passwords exist indefinitely on network devices 1 2 3 4 5
    b. Hardware (h/w) vulnerability
        i. Unsecured physical ports 1 2 3 4 5
        ii. Lack of redundancy for critical networks 1 2 3 4 5
        iii. Inadequate physical protection of network equipment 1 2 3 4 5
        iv. Non-critical personnel have access to equipment & network connections 1 2 3 4 5
    c. Perimeter and Monitoring vulnerability
        i. No security perimeter defined 1 2 3 4 5
        ii. No security monitoring on the ICS network 1 2 3 4 5
        iii. Server unknowingly available on the internet 1 2 3 4 5
        iv. Inadequate, misconfigured, or nonexistent firewall 1 2 3 4 5
    d. Communication vulnerability
        i. Lack of integrity checking for communications 1 2 3 4 5
        ii. Critical monitoring and control paths are not identified 1 2 3 4 5
        iii. Standard communication protocols are used in plain text 1 2 3 4 5

iv. Authentication of users, data, or devices is substandard/nonexistent 1 2 3 4 5
v. Public information regarding ICS design, maintenance, interconnection, and communication available over the internet 1 2 3 4 5

Section Five (Attack Characteristics):

1. Which category of cybercriminals is a primary threat to ICS systems [Appendix B: Threat Agents]? Please rank 1-5 where 1 is the lowest primary concern and 5 is the highest:

Leisure Cybercriminals 1 2 3 4 5
Industrial Spies 1 2 3 4 5
Foreign Intelligence Services 1 2 3 4 5
Terrorists 1 2 3 4 5
Corporate Raiders/Trusted Insiders 1 2 3 4 5
Professional/Hired Cybercriminals 1 2 3 4 5
Criminal Groups 1 2 3 4 5
Bot-network Operators 1 2 3 4 5
Phishers 1 2 3 4 5
Spammers 1 2 3 4 5
Spyware/Malware Authors 1 2 3 4 5

2. What would be the ultimate motive in attacking ICS? Please rank 1-5 where 1 is the least likely motive and 5 is the most likely:

Challenge/Status 1 2 3 4 5
Political 1 2 3 4 5
Espionage 1 2 3 4 5
Financial/Extortion 1 2 3 4 5
Information Theft 1 2 3 4 5
Damage 1 2 3 4 5
Thrill 1 2 3 4 5
Revenge 1 2 3 4 5

3. Indicate which technique cybercriminals would most likely use to attack ICS systems. Please rank 1-5 where 1 is the least likely used technique and 5 is the most likely:

Script/Fuzzers/Brute force attack 1 2 3 4 5
Social engineering/Password theft/Dumpster Diving 1 2 3 4 5
Toolkit 1 2 3 4 5
Use of system as distribution system for other cybercrimes 1 2 3 4 5
Physical control/attack 1 2 3 4 5
IP Spoofing 1 2 3 4 5
Information theft 1 2 3 4 5
Malware 1 2 3 4 5
User command 1 2 3 4 5
Information compromise/Protocol reverse engineering 1 2 3 4 5
Viruses or Worms 1 2 3 4 5
DDoS 1 2 3 4 5
Data manipulation 1 2 3 4 5
System scan 1 2 3 4 5
Spyware 1 2 3 4 5

Section Six (Consequence, Interconnectedness and Interdependencies):

1. Which consequence of an ICS attack would have the greatest impact on electricity services [Appendix C: Consequence]? Please rank 1-5 where 1 is the least impact and 5 is the greatest:

   Corruption of Information 1 2 3 4 5 — Denial/Disruption of Service 1 2 3 4 5
   Inaccurate Information Processing 1 2 3 4 5 — Theft of Service 1 2 3 4 5
   Modification/Tampering of Safety Settings and/or System Configurations 1 2 3 4 5

2. Which consequence of an ICS attack in the electricity sector would be most devastating? Please rank 1 as least devastating and 5 as most:

   Physical (plant equipment) 1 2 3 4 5 — Financial 1 2 3 4 5
   Environmental 1 2 3 4 5 — Operations 1 2 3 4 5
   Safety and Health 1 2 3 4 5 — Legal 1 2 3 4 5

3. Which of the following would be a desirable consequence (for a cybercriminal) of an ICS attack? Please rank 1-5 where 1 is the least desirable consequence and 5 is the most:

   Denial of Electric and Power Services to the public 1 2 3 4 5
   Disruption of the following interconnected infrastructures:
   Transportation 1 2 3 4 5 — Banking & ATMs 1 2 3 4 5
   Running Water 1 2 3 4 5 — Healthcare Services 1 2 3 4 5
   Water Contamination 1 2 3 4 5 — Postal Services 1 2 3 4 5
   Communication Services 1 2 3 4 5 — Emergency Services 1 2 3 4 5
   Sewage Removal and Processing 1 2 3 4 5 — Law Enforcement 1 2 3 4 5

Section Seven (Response and Recovery):

1. Which policing body would cybercriminals be *most worried about* if they were detected (Circle all the apply and then rank 1-5 where 1 is the least threatening to the attacker and 5 is the most threatening)?

CERT (Computer Emergency Response Team) 1 2 3 4 5
FBI (Federal Bureau of Investigation) 1 2 3 4 5
DHS (Department of Homeland Security) 1 2 3 4 5
FCC (Federal Communications Commission) 1 2 3 4 5
CIA (Central Intelligence Agency) 1 2 3 4 5
Secret Service 1 2 3 4 5
Military 1 2 3 4 5
Police Department 1 2 3 4 5
Private Security Firms 1 2 3 4 5

2. Which policing body would cybercriminals *expect to respond* if they were detected (Circle all that apply and then rank 1-5 where 1 is the least likely to respond and 5 is the most likely)?

CERT (Computer Emergency Response Team) 1 2 3 4 5
FBI (Federal Bureau of Investigation) 1 2 3 4 5
DHS (Department of Homeland Security) 1 2 3 4 5
FCC (Federal Communications Commission) 1 2 3 4 5
CIA (Central Intelligence Agency) 1 2 3 4 5
Secret Service 1 2 3 4 5
Military 1 2 3 4 5
Police Department 1 2 3 4 5
Private Security Firms 1 2 3 4 5

3. How quickly would cybercriminals expect a response team to *detect* their attack (Circle one)? instantly; few hours; few days; 1 week; > 1 week

4. How quickly would cybercriminals expect a response team to *diffuse* the attack (Circle one)? instantly; few hours; few days; 1 week; > 1 week
5. If detected, which path would cybercriminals most likely choose (Circle one)? Stop all attacks; Stop attacks to resume later; Minimize intensity; Try a different technique; Continue with same intensity

6. Once the attack has ceased/been stopped, how much time do cybercriminals expect to pass before disrupted services resume normal functionality (Circle one)? instantly; few hours; few days; 1 week; > 1 week

Section Eight (Security Testing, Assessment, and Audits):

1. Do cybercriminals think there is an adequate security policy for ICS? Yes/No
2. Do cybercriminals think there is an adequate formal ICS security training and awareness program? Yes/No
3. Do cybercriminals think there are adequate administrative mechanisms in place for security enforcement? Yes/No
4. Do cybercriminals think security testing is productive in reducing cyberattacks? Yes/No
5. How frequently do cybercriminals think security testing is done (Circle one)? daily; weekly; monthly; quarterly; semi-annually; annually; < 1/year; never
6. Do cybercriminals think vulnerability assessment protocols are productive in reducing cyberattacks? Yes/No
7. How frequently do cybercriminals think vulnerability assessments are conducted (Circle one)? Daily; weekly; monthly; quarterly; semi-annually; annually; less than once a year; never
8. Do cybercriminals think there are independent security audits on the ICS, which determine the adequacy of system controls, detect breaches in security services, and recommend modifications? Yes/No

Section Nine (Knowledge and Alliances):

1. Do cybercriminals access 'ICS hacking' forums? Yes/No
2. Do cybercriminals discuss ICS hacking tips with each other? Yes/No
3. How often do cybercriminals need to revise their ICS hacking skills and knowledge base (Circle one)? 0-10 hrs/wk; 11-20 hrs/wk; 21-30 hrs/wk; 31-40 hrs/wk; 40+ hrs/wk
4. How much money do cybercriminals spend on their attacks (Circle one)? $0-50; $51-150; $151-500; $500-1000; $1001+
5. Do cybercriminals use/convert security testing tools designed for ICS to hone their skills? Yes/No
6. Are cybercriminals more likely to develop their own tools to target ICS or do they rent/buy them elsewhere? (Circle one): Develop own tools/ Rent or buy
7. Are cybercriminals more likely work alone or in partnerships when targeting ICS (Circle one)? Alone, small groups, networks
8. If cybercriminals work in alliances, where do they find their partners, and which partnership is more threatening (Circle all that apply and then rank 1-5 where 1 is the least threatening and 5 is the most)?
   Past successful alliance members 1 2 3 4 5
   Online hacking communities/forums 1 2 3 4 5
   Personal contacts (online and offline) 1 2 3 4 5
   Referrals through other cybercriminals 1 2 3 4 5

Section Ten (Overall Vulnerability Assessment):

1. Which vulnerability poses the most risk? Please rank 1 as lowest and 5 as highest:

Accessibility 1 2 3 4 5	Interconnectedness and interdependencies 1 2 3 4 5
Countermeasures 1 2 3 4 5	Response and recovery 1 2 3 4 5
System weaknesses 1 2 3 4 5	Security testing, assessments, and audits 1 2 3 4 5
Attack characteristics 1 2 3 4 5	Knowledge and alliances 1 2 3 4 5
Consequence 1 2 3 4 5	

2. Which category of vulnerabilities leads to higher threats of attacks? Please rank 1 as lowest and 5 as highest:
    a. Preventative (countermeasures, security testing, assessments, and audits) 1 2 3 4 5
    b. System (accessibility, system weaknesses) 1 2 3 4 5
    c. Reactive (response and recovery) 1 2 3 4 5
    d. Attack (attack characteristics, knowledge and alliances) 1 2 3 4 5
    e. Result (consequence, interconnectedness, and interdependencies) 1 2 3 4 5

3. Which combined vulnerabilities result in the greatest and smallest risk? Please list the numbers of the most likely combination (*example*: (i) + (iii) = greatest risk): (i) accessibility, (ii) countermeasures, (iii) system weaknesses, (iv) attack characteristics, (v) consequence, interconnectedness, and interdependencies, (vi) response and recovery, (vii) security testing, assessments, and audits, (viii) knowledge and alliances. Greatest risk: _____ Smallest risk: _____

Section Eleven (Detailed feedback):

1. Does this survey reflect ICS attacks faithfully? Yes/No
2. Does this survey capture all dimensions of ICS attacks? Yes/No
3. Does this survey capture all dimensions of cybercriminals? Yes/No
4. Which components and/or questions would you like to see revised? Why? What would these revisions entail (Please use reverse side for comments)?

Appendix I: ICS Vulnerabilities (adapted from NIST Guide to Industrial Control Systems Security 800-82) (§ 4-4 & § 4-5)

	Platform Vulnerability	Description
Configuration Vulnerability	Operating System (OS) and security patches are not developed until significantly after security vulnerabilities are found	Because ICS software is complex, any modifications to the underlying OS must undergo comprehensive testing. The elapsed time for such testing and subsequent distribution of updates software provides a long window of vulnerability
	OS and security patches are not maintained	Out-of-date OS and security patches may contain newly discovered vulnerabilities that could be exploited. Security patch support may not even be available for ICS that use outdated OSs.
	OS and security patches are implemented without thorough testing	OS and security patches deployed without testing could compromise normal operation of the ICS.
	Poor password practices (no password used, password disclosure)	Passwords should be implemented to prevent unauthorized access for system login. Passwords should be kept confidential; disclosing passwords via posting them in plain sight, sharing passwords with associates, and sending unencrypted passwords through unprotected communications can lead to unauthorized access.
H/w Vulnerability	Unauthorized personnel have physical access to equipment	Physical access to ICs equipment should be restricted to only the necessary personnel; improper access can lead to physical theft/damage/destruction of data and hardware; unauthorized changes to the functional environment; and undetectable interception of data.
	Insecure remote access on ICS components	Modems and other remote access capabilities that enable operators to gain remote access to ICs should be deployed with security controls to prevent unauthorized access.
	Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the ICS and could create an unsafe situation. Loss of power could also lead to insecure default settings.
	Lack of redundancy for critical components	Lack of redundancy in critical components could provide a single point of failure possibilities.
S/w Vulnerability	Buffer overflow	Cybercriminals could exploit ICS software that is vulnerable to buffer overflows.
	Poor or nonexistent denial of service (DoS) protection	ICS software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.
	Use of proprietary software that has been discussed at conferences and in periodicals	Propriety software issues are discussed at international, IT, ICS, and hacker conferences and are available through technical papers, periodicals, and listervers. This information can help cybercriminals create successful attacks against ICS.
	Inadequate authentication and access control for software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.
	Intrusion detection/prevention software not installed/maintained	IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with works.
	Poor or nonexistent virus protection	Substandard or nonexistent virus protection software can result in the introduction of malware, which results in performance degradation, loss of system availability, and the capture, modification, and deletion of data.
	Poor or nonexistent file integrity checking	Substandard or nonexistent file integrity checking software can result in infected files and programs, which disrupts ICS

		functionality.
	Network Vulnerability	**Description**
Configuration Vulnerability	Weak network security architecture	The ICS network infrastructure has been developed based on business and operational requirements, with little consideration for security. Over time, security gaps may have occurred inadvertently within particular parts of the network, which may represent backdoors into the ICS.
	Passwords not encrypted in transit	Passwords transmitted in clear text across communication systems are susceptible to eavesdropping by cybercriminals, who could reuse them to gain unauthorized access and disrupt ICS operations or to monitor ICS network activity.
	Passwords exist indefinitely on network devices	Passwords not changed regularly can be used by unauthorized parties to disrupt ICS operations or to monitor ICS network activity.
	Inadequate access controls applied	Unauthorized access to network devices and administrative functions could allow cybercriminals to disrupt ICS operations or to monitor ICS network activity.
H/w Vulnerability	Inadequate physical protection of network equipment	Access to network equipment should be controlled to prevent damage or destruction.
	Unsecured physical ports	Unsecured USB and PS/2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.
	Non-critical personnel have access to equipment and network connections	Unauthorized access to network equipment can lead to physical theft/damage/destruction of data and hardware; unauthorized changes to the security environment; and undetectable interception and manipulation of network activity.
	Lack of redundancy for critical networks	Lack of redundancy in critical networks could provide single point of failure possibilities.
Perimeter & Monitoring Vulnerability	No security perimeter defined	If the control network has no security perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly.
	Inadequate, misconfigured, or nonexistent firewall	Inadequate, misconfigured, or nonexistent firewalls could permit unnecessary data to pass between networks, which could result in allowing attacks and malware to spread between networks, making sensitive data susceptible to eavesdropping on other networks, and providing cybercriminals with unauthorized access to systems.
	No security monitoring on the ICS network	Without regular security monitoring, incidents might go unnoticed, leading to additional damage/disruption.
	Server unknowingly available on the internet	Servers may be available on the internet without operator knowledge, rendering the network free to be accessed by cybercriminals.
Communicati	Lack of integrity checking for communications	Cybercriminals could manipulate communications that have no integrity checks; these manipulations can go undetected.
	Critical monitoring and control paths are not identified	Rogue and/or unknown connections into the ICS can leave a backdoor for attacks.
	Standard communication protocols are used in plain text	Cybercriminals can monitor ICS network activity and use a protocol analyzer to decode the data transferred by protocols

		such as telnet, File Transfer Protocol (FTP), and Network File System (NFS), making it easier to perform ICs attacks and manipulate ICs network activity.
	Authentication of users, data, or devices is substandard/ nonexistent	Many ICS protocols have no authentication, allowing cybercriminals to replay, modify, or spoof data.
	Public information regarding ICS design, maintenance, interconnection, and communication available over the internet	The online availability of ICS documentation allows cybercriminals with even little knowledge of ICs to gain unauthorized access to an ICs with the use of automated attacks, data mining tools, and factory-set default passwords that are often not changed.

Appendix II: Threat Agents (adapted from NIST Guide to Industrial Control Systems Security 800-82) (§ 5-1)

Threat Agent	Description
Leisure Cybercriminals	Leisure cybercriminals break into networks for the thrill of the challenge or for bragging rights in the cybercriminal community. While remote cracking once required technical knowhow, leisure cybercriminals can now download attack scripts to launch attacks against ICS. While attack tools have become more sophisticated, they have also become easier to use. Many leisure cybercriminals do not have the required skills to threaten critical infrastructures. However, they still pose a relatively high threat of an isolated or brief disruption causing serious damage.
Industrial Spies	Industrial espionage seeks to acquire intellectual property and knowhow through covert methods.
Foreign Intelligence Services	Foreign intelligence services use cyberattacks for their information gathering and espionage activities. Several nations are developing information warfare doctrines, programs, and capabilities, that can have a major impact by disrupting the supply, communications, and economic infrastructures that support ICS in several infrastructures.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructure to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware to gather sensitive information and may attack one target to divert attention or resources from other targets.
Corporate Raiders/ Trusted Insiders	The disgruntled insider may not need in-depth knowledge about computer intrusions as their knowledge of the ICS often permits them to gain unrestricted access to cause system damage or steal sensitive information. Insiders may be employees, contractors, or business partners. The insider threat also includes employees who accidently introduce malware into systems.
Professional/ Hired Cybercriminals	Professional cybercriminals have a high degree of technical acumen, access to state of the art equipment, and used their technical expertise to further their own criminal pursuits. They are motivated by money, but they either use their skills to attack their chosen targets, or work for organized crime groups as employees, rather than renting/selling their products in the underground economy.
Criminal Groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and malware to conduct their attacks. Criminal groups may hire or develop cybercriminal talent to target ICS. Some criminal groups may try to extort money from an infrastructure sector by threatening a cyberattack.

Bot-network Operators	Bot-network operators are cybercriminals that take over multiple systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. Once these systems are compromised, they may also be made available in the underground economy for rent or sale.
Phishers	Phishers are cybercriminals or small criminal groups that execute phishing schemes to steal identities or information for monetary gain. Phishers may use spam and spyware/malware.
Spammers	Spammers are cybercriminals that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations via DDoS attacks
Spyware/malware authors	Spyware/malware authors have the malicious intent to execute attacks by producing and distributing spyware and malware, such as Nimda, Code Red, Slammer, and Blaster

Appendix III: Consequence (adapted from NIST Guide to Industrial Control Systems Security 800-82) (§ 6-1)

Consequence	**Description**
Corruption of Information	Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
Inaccurate Information Processing	Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.
Theft of Service	Theft of ICS services resulting in the availability of free electricity to the attackers, and possibly cutting off resources to legitimate consumers, causing the infrastructure monetary loss and disruption of service.
Denial/Disruption of Service	Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.
Modification/Tampering of Safety Settings and/or System Configurations	ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects. Interference with the operation of safety systems, which could endanger human life.

Appendix B: Interview Guide - Hackers

Opening Script

I want to thank you for taking the time to speak with me today. <*Read Assent Script for Interviews*>

Background

1. How long have you been working as a hacker?
2. What led you to this work? What were you doing before you came here? What attracted you to hacking/penetration testing?
3. Tell me about your work…
4. How large or well-developed is the group that is responsible for targeting/penetrating (electricity) ICS?
5. What experience do you have targeting/penetrating (electricity) ICS?

Threats, Vulnerabilities and Risks (TVR)

1. There are a lot of different definitions for threats, vulnerabilities and risks (TVR). How would you define these terms? And how are they (if at all) related?
2. Do you think electricity ICS has any particular system vulnerabilities that make them more attractive for attack? What are they?
3. How do you think the situation has changed over the years with respect to vulnerabilities, threats, and risks – has there been an evolution or drastic change?

Perception Differences

1. How would hackers and industry think differently about (electricity) ICS TVR?
2. How would they think the same about TVR?
3. Why would their perceptions differ?
4. What would make their perceptions become the same?

Attacks

1. It has been suggested that the electricity sector is a low-frequency, high-impact target. Do you think this is true? Why (not)?
2. What do you think 'attacking' electricity ICS entails (theft/denial/disruption of service)?
3. Are some techniques preferred over others? Why?
4. What types of people or groups are most involved in hacking electricity ICS? And why would they target these systems? Do they need to be technologically adept?
5. How big of a factor is social engineering when it comes to designing and executing an attack? At what levels/positions does this issue typically become relevant?
6. How do potential offenders become aware of ICS vulnerabilities?
7. When potential offenders are deciding which system to attack, what would possibly be going on in their minds in-terms of a cost-benefit analysis? What do they want to see and what do they don't want to see?

8. If you were to attack an electricity ICS, how would you go about doing it? Please feel free to talk about the planning, development, execution, and aftermath of the attack.
9. Do you think that in the case of an attack, the industry and attackers would ever engage in an attack-response-counterattack-counterresponse cycle? Why (not)?

Response

1. How would cybercriminals deal with industry responses? Are there certain strategies with respect to reassessing the situation, revising the attack, forming new alliances etc?
2. How persistent would cybercriminals be in their attacks? What factors would influence their decision to be persistent? (ex: expenses, skills, time, resources, etc)
3. What causes hackers to stop/delay attacks?
4. How do hackers anticipate the industry's response?

Case Examples

Current events: Stuxnet

1. Stuxnet has been discussed in-depth already by the technological community. But I would like to have your take on it. Could you tell me about Stuxnet?
2. What makes Stuxnet different from previous situations?
3. How sophisticated is the Stuxnet computer program (given that it used 4 zero-day exploits)? What makes this malware important?
4. How many people do you think were involved in the design and implementation of Stuxnet? How did they find each other?
5. What skills were necessary to design this malware? How expensive would it have been to recruit individuals with these skills?
6. It has been speculated that the 4 zero-day exploits may have been bought on the black market – how much does one such exploit cost? How accessible are these online black markets?
7. How long do you think it took to develop Stuxnet? What stages were involved in its development??
8. How do you think the hacking community is responding to/receiving the program? Has it changed anything in terms of strategies, alliances, resources, etc?
9. Do you think this malware will have a version 2.0? What may it look like?
10. How do you think Stuxnet will change the future of ICS attacks? What will these attacks look like?

Past events

1. Can you tell me about past publicized attacks against the electricity ICS
2. How did the hacking community see these attacks?

Current Events
Security specialist Luigi Auriemma recently released a list of 35 vulnerabilities in SCADA products by Siemens Tecnomatix (FactoryLink), Iconics (Genesis 32 and 64), 7-Technologies (IGSS) and DATAC (RealWin). He says that "SCADA is a critical field but nobody really cares about it".

1. Does his comment have value?
2. The 35 vulnerabilities listed were unknown – how do you think this will influence cybercriminals? How long would it take for these vulnerabilities to be exploited?
3. Can these be used to design new attacks? What would these look like?
4. What impact does the release of this type of information have on potential attackers?
5. While this information was released with the best of intentions, is similar information released for malicious purposes? Where may it be released? How accessible is this information?

Closing
Is there anything more you would like to add?

I'll be analyzing the information you and others gave me and using it towards my PhD research. I'll be happy to send you a copy to review at that time, if you are interested.

Thank you for your time.

Appendix C: Interview Guide - Industry

Opening Script

I want to thank you for taking the time to speak with me today. <*Read Assent Script for Interviews*>

Background

1. How long have you been employed in the electricity sector?
2. What led you to this job? What were you doing before you came here? What attracted you to work for the electricity sector?
3. Tell me about your work…
4. How large or well-developed is the group that is responsible for protecting (electricity) ICS?
5. What experience do you have protecting (electricity) ICS?

Threats, Vulnerabilities and Risks (TVR)

1. There are a lot of different definitions for threats, vulnerabilities and risks (TVR). How would you define these terms? And how are they (if at all) related?
2. Do you think electricity ICS has any particular system vulnerabilities that make them more attractive for attack? What are they?
3. How do you think the situation has changed over the years with respect to vulnerabilities, threats, and risks – has there been an evolution or drastic change?

Perception Differences

1. How would hackers and industry think differently about (electricity) ICS TVR?
2. How would they think the same about TVR?
3. Why would their perceptions differ?
4. What would make their perceptions become the same?

Attacks

1. It has been suggested that the electricity sector is a low-frequency, high-impact target. Do you think this is true? Why (not)?
2. What do you think 'attacking' electricity ICS entails (theft/denial/disruption of service)?
3. Are some techniques preferred over others? Why?
4. What types of people or groups are most involved in hacking electricity ICS? And why would they target these systems? Do they need to be technologically adept?
5. How big of a factor is social engineering when it comes to designing and executing an attack? At what levels/positions does this issue typically become relevant?
6. How do potential offenders become aware of ICS vulnerabilities?
7. When potential offenders are deciding which system to attack, what would possibly be going on in their minds in-terms of a cost-benefit analysis? What do they want to see and what do they don't want to see?

8. If you were to attack an electricity ICS, how would you go about doing it? Please feel free to talk about the planning, development, execution, and aftermath of the attack.
9. Do you think that in the case of an attack, the industry and attackers would ever engage in an attack-response-counterattack-counterresponse cycle? Why (not)?

Security Testing, Assessments, and Audits

1. How often (and correspondingly how useful) are security testing and assessments done?
2. Is there a party responsible for auditing these systems? What are they checking for? What are the penalties for failing audits – are they effective?
3. Are simulation exercises done/useful?
4. It has been suggested that ICS vendors are responsible for patches and upgrades, and that if ICS operators install patches on their own they do not receive assistance from ICS vendors – what do you think about this issue?
5. How much time and resources do you think should be spent on security? How does this compare with what is currently being used on security?

Response

1. How would industry deal with ICS attacks? Are there typically security policies and incident-response measures set in place?
2. If an electricity facility detected an attack, what action would it take?
3. What parties would typically be involved in deflecting an attack?
4. How would these parties respond to the attack? (ex: management vs. plant operator)?

Case Examples

Stuxnet

1. Stuxnet has been discussed in-depth already by the technological community. But I would like to have your take on it. Could you tell me about Stuxnet?
2. What makes Stuxnet different from previous situations?
3. How sophisticated is the Stuxnet computer program (given that it used 4 zero-day exploits)? What makes this malware important?
4. How many people do you think were involved in the design and implementation of Stuxnet? How did they find each other?
5. What skills were necessary to design this malware? How expensive would it have been to recruit individuals with these skills?
6. It has been speculated that the 4 zero-day exploits may have been bought on the black market – how much does one such exploit cost? How accessible are these online black markets?
7. How long do you think it took to develop Stuxnet? What stages were involved in its development??
8. How do you think the industry is dealing with this case? Has it changed anything in terms of security, testing, responses, and resources?
9. Do you think this malware will have a version 2.0? What may it look like?
10. How do you think Stuxnet will change the future of ICS attacks? What will these attacks look like?

Past events

1. Can you tell me about past publicized attacks against the electricity ICS
2. How did the industry manage these attacks?

Current Events

Security specialist Luigi Auriemma recently released a list of 35 vulnerabilities in SCADA products by Siemens Tecnomatix (FactoryLink), Iconics (Genesis 32 and 64), 7-Technologies (IGSS) and DATAC (RealWin). He says that "SCADA is a critical field but nobody really cares about it".

1. Does his comment have value?
2. The 35 vulnerabilities listed were unknown – how do you think this will change industry and vendors? How long would it take for these vulnerabilities to be addressed?
3. Can these be used to design new attacks? What would these look like?
4. What impact does the release of this type of information have on potential attackers?
5. While this information was released with the best of intentions, is similar information released for malicious purposes? Where may it be released? How accessible is this information?

Closing

Is there anything more you would like to add?

I'll be analyzing the information you and others gave me and using it towards my PhD research. I'll be happy to send you a copy to review at that time, if you are interested.

Thank you for your time.

Appendix D: Second Exploratory Factor Analysis

System Category

The System category included survey items for the 'Ease of Access' and 'System Weaknesses' factors of PARE RISKS. This category had 38 items, and with a pairwise deletion the subjects varied from 277 to 291, which resulted in subject to item ratio of seven cases. For the KMO index of sampling adequacy, values above 0.6 were required for a good factor analysis. The value of 0.847 was good.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.847
Bartlett's Test of Sphericity	Approx. Chi-Square	3029.421
	df	703
	Sig.	.000

The Total Variance Explained Table below identified the initial eigenvalues and proportions of variance explained by each factor. The scree plot for the first EFA on the System category had suggested that five factors were to be retained. The second EFA was therefore done with five fixed factors, which were extracted in the factor solution. Looking at the proportions of variance, the bulk of the variance attributable to the retained factors was explained by the first (general) factor (21% out of 42%) in the initial solution, whereas the variance was slightly more evenly distributed in the rotated solution (13.99%, 9.32%, 9.96%, 3.56%, 11.18%).

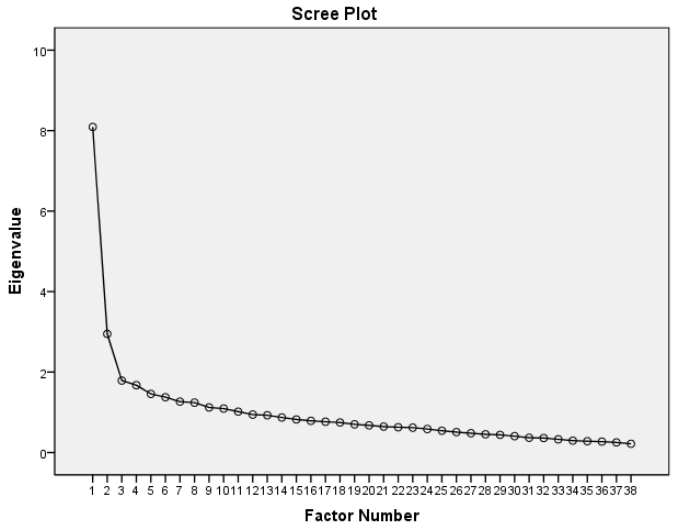
Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]	
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance
1	8.091	21.292	21.292	7.480	19.685	19.685	5.317	13.99211
2	2.949	7.760	29.052	2.410	6.342	26.028	3.543	9.323684
3	1.789	4.709	33.761	1.242	3.270	29.297	3.786	9.963158
4	1.674	4.405	38.166	1.004	2.641	31.938	1.353	3.560526
5	1.457	3.833	41.999	.871	2.293	34.231	4.249	11.18158
6	1.376	3.622	45.621					
7	1.265	3.329	48.950					
8	1.240	3.263	52.214					
9	1.121	2.949	55.163					
10	1.093	2.876	58.040					
11	1.016	2.674	60.714					
12	.944	2.484	63.198					
13	.926	2.436	65.634					
14	.872	2.295	67.929					
15	.822	2.164	70.094					
16	.787	2.072	72.165					
17	.766	2.015	74.180					
18	.747	1.967	76.147					
19	.701	1.844	77.991					
20	.676	1.779	79.770					

21	.645	1.699	81.469
22	.630	1.657	83.125
23	.619	1.628	84.754
24	.585	1.538	86.292
25	.543	1.428	87.720
26	.508	1.337	89.058
27	.480	1.263	90.321
28	.454	1.196	91.517
29	.440	1.158	92.675
30	.407	1.071	93.746
31	.368	.967	94.714
32	.362	.952	95.666
33	.328	.864	96.529
34	.297	.781	97.311
35	.282	.743	98.054
36	.271	.714	98.768
37	.251	.660	99.428
38	.217	.572	100.000

Extraction Method: Principal Axis Factoring.
a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Next, the scree plot gave an indication of how many factors were to be retained. The change in slope, or the 'elbow' was a useful guide. In the plot below, this discontinuity occurred at five factors, and so a five-factor solution was considered.



In order to determine what these factors were, the pattern matrix was analyzed next. The *first* factor was readily interpretable as network security and monitoring and had eight items, with high loadings of network communication vulnerability monitoring not identified (.645), network communication vulnerability lack checking communications (.518), network perimeter monitoring vulnerability no security monitoring (.641), network perimeter monitoring vulnerability no security perimeter (.549), network configuration vulnerability weak network architecture (.571), platform software vulnerability poor file integrity checking (.38), network configuration

vulnerability inadequate access controls (.352), and network configuration vulnerability passwords exist indefinitely (.308).

The *second* factor was readily interpretable as lack of redundancy measures and had three items, with high loadings of platform hardware vulnerability lack of redundancy (-.837), platform hardware vulnerability lack of backup power (-.730), and network hardware lack of redundant networks (-.652). The negative loading implied that the relation between the item and the factor was backwards.

The *third* factor was readily interpretable as non-cyber/physical access and had four items, with high loadings of Network hardware vulnerability inadequate physical protection (.725), platform hardware vulnerability unauthorized personnel access (.677), network hardware vulnerability non critical personnel have access (.666), and network hardware vulnerability unsecured physical ports (.348).

The *fourth* factor was readily interpretable as remote access and had two items, with loadings of virtual private network (-.437) and intranet (-.310). There was another item that loaded on the fourth factor, but had the opposite signatory value: dial up connection (.559). This item was therefore dropped.

The *fifth* factor was readily interpretable as authentication issues and had 11 items, with high loadings of platform configuration vulnerability poor password practices (.650), platform hardware vulnerability insecure remote access (.602), platform software vulnerability inadequate authentication (.535), network perimeter monitoring vulnerability inadequate firewall (.502); network perimeter monitoring vulnerability server available on internet (.466), platform configuration vulnerability OS security patches not maintained (.387), network communication vulnerability substandard authentication (.373), platform hardware vulnerability unauthorized personnel have access (.337), network configuration vulnerability password not encrypted (.336), platform software vulnerability buffer overflow (.327), and platform configuration vulnerability OS security patches not installed after vulnerability known (.315).

This solution did not have factor purity, as some items loaded on more than one factor, so the factors were not clearly defined by the groupings of tests that loaded on them. Additionally, most factors did not have 5 or more strongly loaded items (.50 or better), which would have been desirable and indicative of a solid factor (Costello & Osborne 2005).

Pattern Matrix[a]

	Factor				
	1	2	3	4	5
NetworkCommunicationVulnerabilityMonitoringNotIdentified_9	.645				
NetworkPerimeterMonitoringVulnerabilityNoSecurityMonitoring_9	.641				
NetworkConfigurationVulnerabilityWeakNetworkArchitecture_9	.571				
NetworkPerimeterMonitoringVulnerabilityNoSecurityPerimeter_9	.549				
NetworkCommunicationVulnerabilityLackCheckingCommunications_9	.518				
PlatformSoftwareVulnerabilityPoorFileIntegrityChecking_9	.380				
NetworkConfigurationVulnerabilityInadequateAccessControls_9	.352				.343
NetworkConfigurationVulnerabilityPasswordsExistIndefinitely_9	.308				
PlatformSoftwareVulnerabilityIDSNotMaintained_9					
PlatformSoftwareVulnerabilityPoorVirusProtection_9					
PlatformHardwareVulnerabilityLackRedundancy_9		-.837			
PlatformHardwareVulnerabilityLackBackupPower_9		-.730			
NetworkHardwareVulnerabilityLackRedundantNetworks_9		-.652			
PlatformConfigurationVulnerabilityOSSecurityPatchesWithoutTesting_9					
NetworkCommunicationVulnerabilitySensitiveInformationInternet_9					
PlatformSoftwareVulnerabilityPoorDoSProtection_9					
PlatformSoftwareVulnerabilityUseProprietarySoftware_9					
RemoteAccessFrequency_4					
NetworkHardwareVulnerabilityInadequatePhysicalProtection_9			.725		
PlatformHardwareVulnerabilityUnauthorizedPersonnelAccess_9			.677		.337
NetworkHardwareVulnerabilityNonCriticalPersonnelHaveAccess_9			.666		
NetworkHardwareVulnerabilityUnsecuredPhysicalPorts_9			.348		

RemoteAccessDialupConnection_4				.559	
RemoteAccessVirtualPrivateNetwork_4				-.437	
RemoteAccessIntranet_4				-.310	
RemoteAccessWideAreaNetwork_4					
PlatformConfigurationVulnerabilityPoorPasswordPractices_9					.650
PlatformHardwareVulnerabilityInsecureRemoteAccess_9					.602
PlatformSoftwareVulnerabilityInadequateAuthentication_9					.535
NetworkPerimeterMonitoringVulnerabilityInadequateFirewall_9					.502
NetworkPerimeterMonitoringVulnerabilityServerAvailableInternet_9					.466
PlatformConfigurationVulnerabilityOSSecurityPatchesNotMaintained_9					.387
NetworkCommunicationVulnerabilitySubstandardAuthentication_9					.373
NetworkConfigurationVulnerabilityPasswordNotEncrypted_9					.336
PlatformSoftwareVulnerabilityBufferOverflow_9					.327
PlatformConfigurationVulnerabilityOSSecurityPatchesAfterVulnerability_9					.315
NetworkCommunicationVulnerabilityPlainTextCommunicationProtocols_9					
AttackFrequency_4					

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 26 iterations.

It is worth knowing whether a scale defined by factor loadings is really measuring a unitary construct. The usual index of the internal consistency of a scale is, as noted above, Cronbach's α. As noted earlier, a value between .7 and .8 is an acceptable value for Cronbach's α, although a lenient cut-off of .60 is common in EFA (Field 2005). For the eight items comprising the network security and monitoring factor, Alpha = .81 and the reliability would not be improved by removing any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.810	8

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PlatformSoftwareVulnerabilityPoorFileIntegrityChecking_9	27.28	20.874	.511	.790
NetworkConfigurationVulnerabilityWeakNetworkArchitecture_9	26.69	21.408	.541	.786
NetworkConfigurationVulnerabilityInadequateAccessControls_9	26.79	22.016	.486	.794
NetworkConfigurationVulnerabilityPasswordsExistIndefinitely_9	26.79	21.829	.429	.802
NetworkPerimeterMonitoringVulnerabilityNoSecurityMonitoring_9	26.90	21.256	.545	.785
NetworkPerimeterMonitoringVulnerabilityNoSecurityPerimeter_9	26.91	21.269	.470	.797
NetworkCommunicationVulnerabilityMonitoringNotIdentified_9	27.44	19.900	.633	.771
NetworkCommunicationVulnerabilityLackCheckingCommunications_9	27.37	20.603	.583	.779

For the three items comprising the lack of redundancy measures factor, Alpha = .814 and the reliability would not be improved by removing any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.814	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PlatformHardwareVulnerabilityLackRedundancy_9	5.47	4.171	.728	.677
PlatformHardwareVulnerabilityLackBackupPower_9	5.90	4.245	.672	.737
NetworkHardwareVulnerabilityLackRedundantNetworks_9	5.48	4.939	.599	.808

For the four items comprising the non-cyber/physical access factor, Alpha = .741 and the reliability would be slightly improved by removing the network hardware vulnerability unsecured physical port item (.759).

Reliability Statistics

Cronbach's Alpha	N of Items
.741	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PlatformHardwareVulnerabilityUnauthorizedPersonnelAccess_9	11.42	6.360	.546	.675
NetworkHardwareVulnerabilityInadequatePhysicalProtection_9	11.99	5.913	.644	.617
NetworkHardwareVulnerabilityNonCriticalPersonnelHaveAccess_9	11.67	6.496	.561	.668
NetworkHardwareVulnerabilityUnsecuredPhysicalPorts_9	12.05	6.706	.403	.759

For the two items comprising the remote access factor, α = .349 and the reliability would obviously not be improved by removing any of the items. The α reliability is extremely low, which suggests that there is no real internal consistence in the measurement. However, this factor is still retained as it emerges as a relevant offender decision-making factor in the interviews as well.

Reliability Statistics

Cronbach's Alpha	N of Items
.349	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
RemoteAccessIntranet_4	3.43	1.794	.213	.
RemoteAccessVirtualPrivateNetwork_4	3.75	1.350	.213	.

For the eleven items comprising the authentication factor, Alpha = .810 and the reliability would not be improved by removing any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.810	11

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PlatformConfigurationVulnerabilityPoorPasswordPractices_9	42.75	31.330	.589	.785
PlatformConfigurationVulnerabilityOSSecurityPatchesAfterVulnerability_9	43.45	31.468	.401	.804
PlatformConfigurationVulnerabilityOSSecurityPatchesNotMaintained_9	42.76	32.941	.442	.798
PlatformHardwareVulnerabilityInsecureRemoteAccess_9	43.08	30.910	.537	.789
PlatformHardwareVulnerabilityUnauthorizedPersonnelAccess_9	43.06	30.667	.500	.793
PlatformSoftwareVulnerabilityInadequateAuthentication_9	43.18	31.515	.489	.794
PlatformSoftwareVulnerabilityBufferOverflow_9	43.52	31.675	.391	.805

NetworkPerimeterMonitoringVulnerabilityInadequateFirewall_9	42.92	31.566	.524	.790
NetworkPerimeterMonitoringVulnerabilityServerAvailableInternet_9	42.71	32.304	.528	.791
NetworkCommunicationVulnerabilitySubstandardAuthentication_9	42.87	33.403	.426	.800
NetworkConfigurationVulnerabilityPasswordNotEncrypted_9	43.15	31.631	.442	.799

Thus five factors were retained for the System category: 'Network security & monitoring'; 'Lack of redundancy'; 'Remote Access'; 'Non-cyber/Physical access'; 'Authentication'.

Attacker Category

The Attacker category included survey items for the 'Attacks & Alliances' and 'Knowledge, Skills, Research & Development' factors of PARE RISKS. This category had 23 items, and with a pairwise deletion the subjects varied from 265 to 283, which resulted in subject to item ratio of 11 to 12 cases respectively. For the KMO index of sampling adequacy, values above 0.6 were required for a good factor analysis. The value of 0.720 was good.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.720
Bartlett's Test of Sphericity	Approx. Chi-Square	1420.160
	Df	253
	Sig.	.000

The Total Variance Explained Table below identified the initial eigenvalues and proportions of variance explained by each factor. The scree plot for the first EFA on the Attacker category had suggested that five factors were to be retained. The second EFA was therefore done with five fixed factors, which were extracted in the factor solution. Looking at the proportions of variance, the bulk of the variance attributable to the retained factors was explained by the first (general) factor (16% out of 49%) in the initial solution, whereas the variance was slightly more evenly distributed in the rotated solution (12.71%, 9.27%, 7.48%, 7.32%, 3.37%).

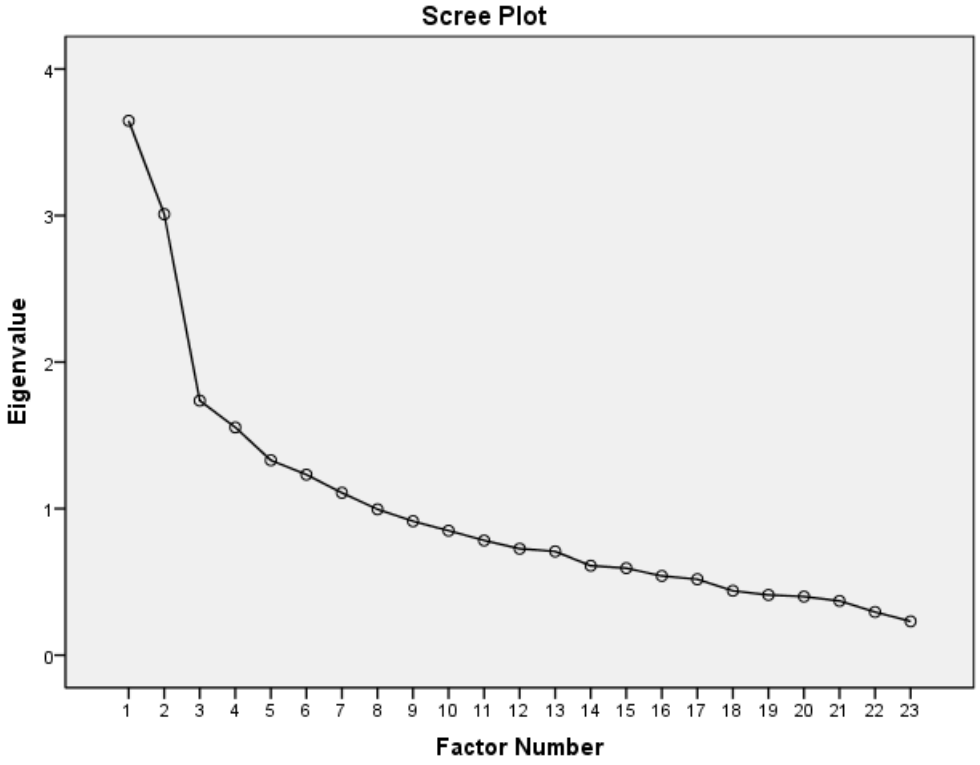
Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]	
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance
1	3.647	15.856	15.856	3.151	13.701	13.701	2.923	12.7087
2	3.009	13.083	28.940	2.436	10.593	24.293	2.133	9.273913
3	1.737	7.552	36.492	1.255	5.456	29.750	1.720	7.478261
4	1.554	6.758	43.250	.916	3.982	33.731	1.684	7.321739
5	1.330	5.781	49.031	.662	2.880	36.611	.774	3.365217
6	1.232	5.356	54.387					
7	1.108	4.817	59.204					
8	.995	4.328	63.532					
9	.914	3.974	67.507					
10	.849	3.693	71.200					
11	.783	3.403	74.603					
12	.727	3.159	77.762					
13	.708	3.079	80.841					
14	.610	2.652	83.493					
15	.594	2.581	86.073					
16	.540	2.349	88.422					
17	.518	2.252	90.674					
18	.439	1.909	92.583					
19	.411	1.787	94.370					
20	.400	1.739	96.108					
21	.370	1.609	97.717					
22	.294	1.280	98.997					
23	.231	1.003	100.000					

Extraction Method: Principal Axis Factoring.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Next, the scree plot gave an indication of how many factors were to be retained. The change in slope, or the 'elbow' was a useful guide. In the plot below, this discontinuity occurred at five factors, and so a five-factor solution was considered.



In order to determine what these factors were, the pattern matrix was analyzed next. The *first* factor was readily interpretable as commercial attacks and had five items, with high loadings of phishers (.839), spammers (.848), spyware malware authors (.689), bot network operators (.570), and information theft (.323).

The *second* factor was readily interpretable as political attacks and had six items, with high loadings of foreign intelligence services (.722), terrorists (.603), espionage (.639), political (.491), damage (.422), and industrial spies (.307).

The *third* factor was readily interpretable as leisure attacks, with high loadings of challenge/status (.835), and thrill (.723). The *fourth* factor was readily interpretable as business-financial attacks and had five items, with loadings of financial extortion (.536), professional/hired cybercriminals (.480), criminal groups (.433), past successful alliances (.429), and corporate raiders/trusted insiders (.373).

The fifth factor was not readily interpretable, as the four items that loaded onto this factor did not share a common theme and also had different signatory values: industrial spies (-.38), criminal groups (.38), espionage (-.396), and revenge (.354). As such, this factor was not retained.

The solution with four factors had factor purity (for loadings >=.3), as each item loaded on only one factor, so that the factors were clearly defined by the groupings of tests that loaded on them. Additionally, all factors did not have 5 or more strongly loaded items (.50 or better), which would have been desirable and indicative of a solid factor (Costello & Osborne 2005).

Pattern Matrix[a]

	Factor				
	1	2	3	4	5
LeisureCybercriminals_2					
IndustrialSpies_2		.307			-.380
ForeignIntelligenceServices_2		.722			
Terrorists_2		.603			
CorporateRaidersTrustedInsiders_2				.373	
ProfessionalHiredCybercriminals_2				.480	
CriminalGroups_2				.433	.380
BotNetworkOperators_2	.570				
Phishers_2	.839				
Spammers_2	.848				
SpywareMalwareAuthors_2	.689				
ChallengeStatus_2			.835		
Political_2		.491			
Espionage_2		.639			-.396
FinancialExtortion_2				.536	
InformationTheft_2	.323				
Damage_2		.422			
Thrill_2			.723		
Revenge_2					.354
AllianceCriteriaPastSuccess_2				.429	
AllianceCriteriaOnlineHackingCommunities_2					
AllianceCriteriaPersonalcontacts_2					
AllianceCriteriaReferrals_2					

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 11 iterations.

It is worth knowing whether a scale defined by factor loadings is really measuring a unitary construct. The usual index of the internal consistency of a scale is, as noted above, Cronbach's α. As noted earlier, a value between .7 and .8 is an acceptable value for Cronbach's α, although a lenient cut-off of .60 is common in EFA (Field 2005). For the four items comprising the commercial factor, Alpha = .791 and the reliability would be improved by the removal of the information theft item (.837).

Reliability Statistics

Cronbach's Alpha	N of Items
.791	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
BotNetworkOperators_2	10.15	14.651	.550	.758
Phishers_2	10.72	13.359	.715	.703
Spammers_2	11.12	14.089	.694	.714
SpywareMalwareAuthors_2	10.47	13.844	.639	.729
InformationTheft_2	9.97	16.853	.295	.837

For the five items comprising the political factor, Alpha = .705 and the reliability would be improved slightly by the removal of the damage item.

Reliability Statistics

Cronbach's Alpha	N of Items
.705	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ForeignIntelligenceServices_2	18.63	15.206	.578	.622
Terrorists_2	18.89	15.628	.470	.655
Political_2	19.02	16.533	.385	.682
Espionage_2	19.02	14.656	.575	.619
Damage_2	18.99	17.440	.292	.710
IndustrialSpies_2	19.05	17.311	.334	.696

For the three items comprising the leisure factor, Alpha = .741 and the reliability would obviously not be improved by the removal of any items.

Reliability Statistics

Cronbach's Alpha	N of Items
.741	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ChallengeStatus_2	3.02	1.626	.590	.
Thrill_2	3.15	1.386	.590	.

For the five items comprising the business-financial factor, Alpha = .604 and the reliability would be improved slightly by the removal of the past successful alliance criteria item (.623).

Reliability Statistics

Cronbach's Alpha	N of Items
.604	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
FinancialExtortion_2	14.91	8.783	.409	.521
ProfessionalHiredCybercriminals_2	14.75	8.648	.486	.482
CriminalGroups_2	15.29	8.680	.415	.518
CorporateRaidersTrustedInsiders_2	15.17	9.598	.294	.583
AllianceCriteriaPastSuccess_2	14.41	10.568	.200	.623

Thus four factors were retained for the Attacker category, namely ‘Commercial’; ‘Political’; ‘Leisure’; ‘Business-Financial’.

Attack Category

The Attack category included survey items for the ‘Attacks & Alliances’ and ‘Knowledge, Skills, Research & Development’ factors of PARE RISKS. This category had 18 items, and with a pairwise deletion the subjects varied from 263 to 285, which resulted in subject to item ratio of 14 to 15 cases respectively. For the KMO index of sampling adequacy, values above 0.6 were required for a good factor analysis. The value of 0.793 was good.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.793
Bartlett's Test of Sphericity	Approx. Chi-Square	780.635
	Df	153
	Sig.	.000

The Total Variance Explained Table below identified the initial eigenvalues and proportions of variance explained by each factor. The scree plot for the first EFA on the Attack category had suggested that five factors were to be retained. The second EFA was therefore done with five fixed factors, which were extracted in the factor solution. Looking at the proportions of variance, the bulk of the variance attributable to the retained factors was explained by the first (general) factor (22% out of 51%) in the initial solution, whereas the variance was slightly more evenly distributed in the rotated solution (14.38%, 8.9%, 5.2%, 4.2%, 12%).

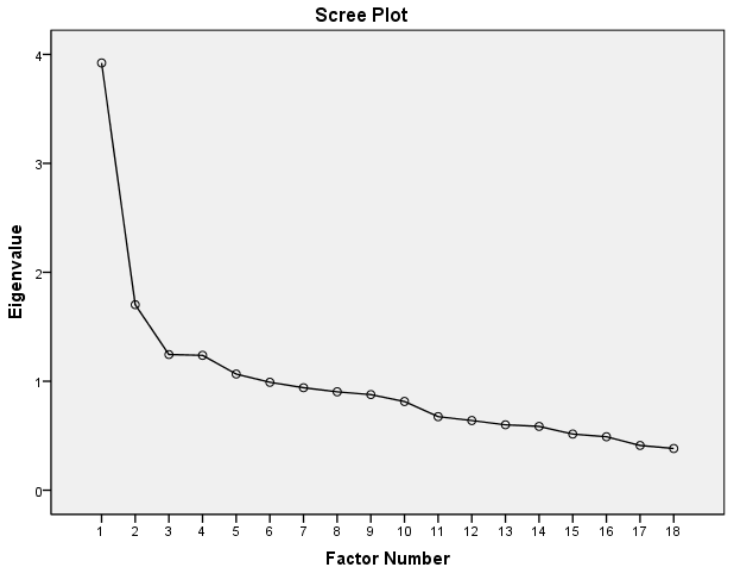
Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]	
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance
1	3.922	21.788	21.788	3.339	18.551	18.551	2.589	14.38333
2	1.703	9.460	31.248	1.085	6.030	24.581	1.596	8.866667
3	1.245	6.918	38.165	.592	3.287	27.868	.940	5.222222
4	1.238	6.876	45.041	.521	2.892	30.761	.747	4.15
5	1.066	5.923	50.964	.421	2.340	33.100	2.155	11.97222
6	.990	5.503	56.466					
7	.941	5.227	61.694					
8	.903	5.019	66.712					
9	.878	4.875	71.588					
10	.814	4.525	76.112					
11	.675	3.750	79.862					
12	.640	3.553	83.415					
13	.600	3.335	86.750					
14	.586	3.254	90.003					
15	.515	2.862	92.865					
16	.491	2.727	95.592					
17	.411	2.282	97.874					
18	.383	2.126	100.000					

Extraction Method: Principal Axis Factoring.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Next, the scree plot gave an indication of how many factors were to be retained. The change in slope, or the 'elbow' was a useful guide. In the plot below, this discontinuity occurred at five factors, and so a five-factor solution was considered.



In order to determine what these factors were, the pattern matrix was analyzed next. The *first* factor was readily interpretable as information-seeking (preliminary target research stage) techniques and had seven items, with loadings of system scan (.721), IP Spoofing (.501), spyware (.438), toolkit (.355), information theft (.323), script fuzzers/brute force attack (.303), and use as distribution system (.303).

The *second* factor was readily interpretable attack-in-progress techniques and had three items, with loadings of data manipulation (.566), physical attack (.492), and information compromise (.423).

The *third* factor was readily interpretable as non-technical techniques and had two items, with loadings of toolkits (-.461) and social engineering/dumpster diving (-.395). A third item that loaded onto this factor was attack expenses (.369), but did not tie into the 'non-technical technique' theme and also had the opposite signatory values than the other items that loaded onto this factor. Hence it was not retained.

The fourth factor was not readily interpretable. The items that loaded onto this factor did not share any common underlying characteristics: use as distribution system and access forums. Furthermore, their loadings had opposite signatory values, with the former loading of -.410 and the latter loading of .314. As such this factor was not included.

The *fifth* factor was readily interpretable as installation techniques (unknown to user) and had three items, with high loadings of viruses and worms (.838), malware (.554) and spyware (.434).

This solution did not have factor purity, as some items did not load highly on just one factor, and so the factors were not clearly defined by the groupings of tests that load on them. Additionally, none of the factors had 5 or more strongly loaded items (.50 or better), which would have been desirable and indicative of a solid factor (Costello & Osborne 2005).

Pattern Matrix[a]

	Factor				
	1	2	3	4	5
ScriptFuzzersBruteForceAttack_2	.303				
SocialEngineeringDumpsterDiving_2			-.395		
Toolkit_2	.355		-.461		
UseAsDistributionSystem_2	.303			-.410	
PhysicalAttack_2		.492			
IPSpoofing_2	.501				
InformationTheftTechnique_2	.323				
Malware_2					.554
UserCommand_2					
InformationCompromise_2		.423			
VirusesWorms_2					.838
DDoS_2					
DataManipulation_2		.566			
SystemScan_2	.721				
Spyware_2	.438				.434
AccesFormus_8				.314	
RevisionFrequency_8					
AttackExpenses_8			.369		

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 16 iterations.

It was worth knowing whether a scale defined by factor loadings was really measuring a unitary construct. The usual index of the internal consistency of a scale was Cronbach's α. It is worth knowing whether a scale defined by factor loadings is really measuring a unitary construct. The usual index of the internal consistency of a scale is, as noted above, Cronbach's α. As noted earlier, a value between .7 and .8 is an acceptable value for Cronbach's α, although a lenient cut-off of .60 is common in EFA (Field 2005).

For the seven items comprising the information-seeking techniques factor, α = .73 and the reliability would not be improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.730	7

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ScriptFuzzersBruteForceAttack_2	18.43	23.428	.336	.722
Toolkit_2	18.38	23.581	.347	.719
UseAsDistributionSystem_2	19.02	21.870	.435	.700
IPSpoofing_2	18.91	22.068	.485	.688
InformationTheftTechnique_2	18.68	22.315	.446	.697
SystemScan_2	18.53	20.865	.522	.678
Spyware_2	19.00	21.008	.519	.679

For the three items comprising the attack-in-progress techniques item, α = .494 and the reliability would not be improved by the removal of any items The α reliability is extremely low, which suggests that there is no real internal consistence in the measurement. However, this factor is still retained as it emerges as a relevant offender decision-making factor in the interviews as well..

Reliability Statistics

Cronbach's Alpha	N of Items
.494	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PhysicalAttack_2	6.73	3.360	.267	.469
InformationCompromise_2	6.47	3.301	.306	.404
DataManipulation_2	6.91	3.089	.364	.303

For the three items comprising the non-technical techniques item, α = .405 and the reliability would obviously not be improved by removal of any of the items. The α reliability is extremely low, which suggests that there is no real internal consistence in the measurement. However, this factor is still retained as it emerges as a relevant offender decision-making factor in the interviews as well.

Reliability Statistics

Cronbach's Alpha	N of Items
.405	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
SocialEngineeringDumpsterDiving_2	3.39	1.399	.255	.
Toolkit_2	4.03	1.108	.255	.

For the three items comprising the installation techniques item, $\alpha = .739$ and the reliability would not be improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.739	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Malware_2	6.27	4.761	.592	.619
VirusesWorms_2	6.10	5.060	.538	.682
Spyware_2	6.73	4.837	.560	.657

Thus four factors were retained for the Attack category, namely 'Information-seeking techniques'; 'Attack-in-progress techniques'; 'Non-technical techniques'; and 'Installation techniques'.

Result Category

The Result category included survey items for the 'Response & Recovery' factor of PARE RISKS. This category had 22 items, and with a pairwise deletion the subjects varied from 256 to 287, which resulted in subject to item ratio of 12 to 13 cases respectively. For the KMO index of sampling adequacy, values above 0.6 were required for a good factor analysis. The value of 0.767 was good.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.767
Bartlett's Test of Sphericity	Approx. Chi-Square	1530.406
	df	210
	Sig.	.000

The Total Variance Explained Table below identified the initial eigenvalues and proportions of variance explained by each factor. The scree plot for the first EFA on the Result category had suggested that six factors were to be retained. The second EFA was therefore done with six fixed factors, which were extracted in the factor solution.

Looking at the proportions of variance, the bulk of the variance attributable to the retained factors was explained by the first (general) factor (23% out of 60%) in the initial solution, whereas the variance was slightly more evenly distributed in the rotated solution (16.8%, 7.1%, 7.2%, 14.31%, 5.39%, 7.4%).

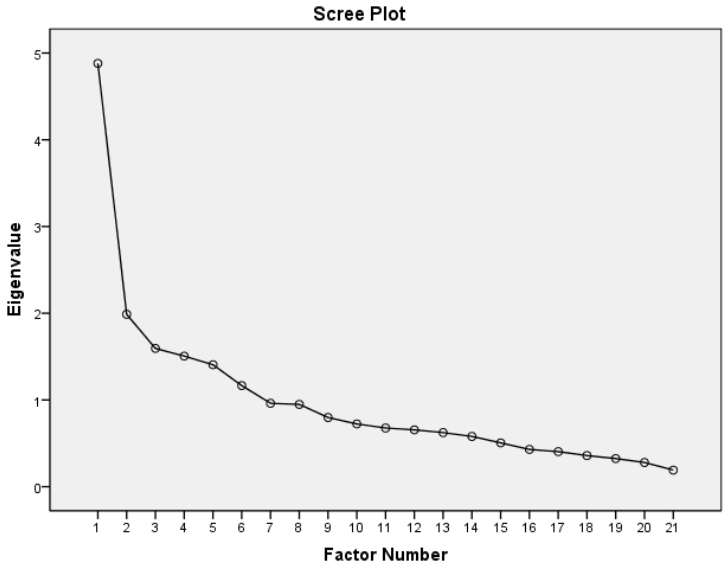
Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]	
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance
1	4.881	23.242	23.242	4.415	21.022	21.022	3.528	16.8
2	1.988	9.465	32.707	1.485	7.072	28.094	1.492	7.104762
3	1.594	7.593	40.300	1.027	4.889	32.983	1.511	7.195238
4	1.506	7.171	47.471	.994	4.734	37.717	3.005	14.30952
5	1.406	6.696	54.167	.799	3.805	41.521	1.131	5.385714
6	1.166	5.553	59.719	.594	2.827	44.348	1.553	7.395238
7	.962	4.580	64.299					
8	.949	4.520	68.819					
9	.798	3.799	72.618					
10	.723	3.444	76.062					
11	.677	3.222	79.285					
12	.655	3.118	82.403					
13	.624	2.971	85.374					
14	.579	2.759	88.133					
15	.505	2.406	90.539					
16	.429	2.045	92.584					
17	.404	1.924	94.508					
18	.359	1.710	96.219					
19	.324	1.544	97.762					
20	.278	1.326	99.089					
21	.191	.911	100.000					

Extraction Method: Principal Axis Factoring.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Next, the scree plot gave an indication of how many factors were to be retained. The change in slope, or the 'elbow' was a useful guide. In the plot below, this discontinuity occurred at six factors, and so a six-factor solution was considered.



In order to determine what these factors were, the pattern matrix was analyzed next. The *first* factor was readily interpretable as disrupting human health related dependent infrastructures and had four items, with loadings of running water (.887), water contamination (.876), sewage removal processing (.666), and healthcare services (.347). Another item loaded on this factor, but was dropped because it did not relate with the other items: transportation (.455).

The *second* factor was readily interpretable as information-related consequence on the electricity sector and had two items, with loadings of inaccurate information processing (.749), and information corruption (.652).

The *third* factor was readily interpretable as devastating environmental and health consequence and had two items, with loadings of environmental impact (.707), and safety and health (.526). Another item loaded onto this factor, but did not fit with the environmental and health theme and also had the opposite signatory value as other items: plant operations (-.306). As such, this item was dropped.

The *fourth* factor was readily interpretable as order and finance and had four items, with high loadings of law enforcement (.766), emergency services (.642), banking (.579), and communication services (.483). Another item loaded onto this factor, but did not fit with the order and finance theme as other items: health care services (.4). As such, this item was dropped.

The *fifth* factor was readily interpretable as plant operations and had four items, with modifying safety settings (.612), plant operations (.435), disrupting physical plant (.311), and denial/disruption of service (.303).

The sixth factor was not readily interpretable all the items that loaded on this factor did not have any common underlying factor: legal (.531), financial (.461), theft of service (.452); plant operations (.318) and postal services (.324). As such, this factor was not retained.

This solution did not have factor purity, as some items did not load highly on just one factor, and so the factors were not clearly defined by the groupings of tests that load

on them. Additionally, none of the factors had 5 or more strongly loaded items (.50 or better), which was desirable and indicative of a solid factor (Costello & Osborne 2005).

Pattern Matrix[a]

	Factor					
	1	2	3	4	5	6
InterconnectednessInterdependencyRunningWater_6	.887					
InterconnectednessInterdependencyWaterContamination_6	.876					
InterconnectednessInterdependencySewageRemovalProcessing_6	.666					
InterconnectednessInterdependencyTransportation_6	.455					
ConsequenceImpactInaccurateInformationProcessing_3		.749				
ConsequenceImpactInformationCorruption_3		.652				
ConsequenceDevastatingEnvironmental_3			.707			
ConsequenceDevastatingSafetyHealth_3			.526			
InterconnectednessInterdependencyLawEnforcement_6				.766		
InterconnectednessInterdependencyeEmergencyServices_6				.642		
InterconnectednessInterdependencyBankingATM_6				.579		
InterconnectednessInterdependencyCommunicationServices_6				.483		
InterconnectednessInterdependencyHealthcareServices_6	.347			.400		
ConequenceImpactModificationSafetySettingsSystemConfigurations_3					.612	
ConsequenceDevastatingOperations_3			-.306		.435	.318
ConsequenceDevastatingPhysicalPlant_3					.311	
ConsequenceImpactDenialDisruptionService_3					.303	
ConsequenceDevastatingLegal_3						.531
ConsequenceDevastatingFinancial_3						.461
ConsequenceImpactTheftService_3						.452
InterconnectednessInterdependencyPostalServices_6						.324

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 13 iterations.

It is worth knowing whether a scale defined by factor loadings is really measuring a unitary construct. The usual index of the internal consistency of a scale is, as noted

above, Cronbach's α. As noted earlier, a value between .7 and .8 is an acceptable value for Cronbach's α, although a lenient cut-off of .60 is common in EFA (Field 2005).

For the five items comprising the disrupting human health related dependent infrastructures, $\alpha = .843$ and the reliability would not be improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.843	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
InterconnectednessInterdependencyTransportation_6	12.16	22.030	.535	.839
InterconnectednessInterdependencyRunningWater_6	12.25	18.611	.797	.768
InterconnectednessInterdependencyWaterContamination_6	12.38	18.331	.754	.780
InterconnectednessInterdependencySewageRemovalProcessing_6	12.98	20.741	.623	.817
InterconnectednessInterdependencyHealthcareServices_6	12.72	21.508	.541	.839

However, because transportation and health care items do not fit with the remaining items, they are dropped. This results in a slightly improved $\alpha = .846$ and the reliability would not be drastically improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.846	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
InterconnectednessInterdependencyRunningWater_6	5.89	6.810	.732	.766
InterconnectednessInterdependencyWaterContamination_6	6.01	6.123	.785	.711
InterconnectednessInterdependencySewageRemovalProcessing_6	6.61	7.620	.628	.861

For the two items comprising the information-related consequence on the electricity sector item, $\alpha = .732$ and the reliability would not be improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.732	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ConsequenceImpactInformationCorruption_3	3.17	1.236	.578	.
ConsequenceImpactInaccurateInformationProcessing_3	3.19	1.354	.578	.

For the three items comprising the devastating environmental and health consequence on the electricity sector, $\alpha = .284$ and the reliability would be improved by removal of the plant operations item.

Reliability Statistics

Cronbach's Alpha	N of Items
.284	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ConsequenceDevastatingEnironmental_3	7.26	2.848	.317	-.155[a]
ConsequenceDevastatingSafetyHealth_3	7.11	2.642	.301	-.154[a]
ConsequenceDevastatingOperations_3	7.04	4.513	-.083	.652

a. The value is negative due to a negative average covariance among items. This violates reliability model assumptions. You may want to check item codings.

After removing the item, $\alpha = .644$ and the reliability would obviously not be improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.644	2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ConsequenceDevastatingEnvironmental_3	3.60	1.617	.476	.
ConsequenceDevastatingSafetyHealth_3	3.43	1.420	.476	.

For the five items comprising the order and finance factor, $\alpha = .781$ and the reliability would not be improved by removal of any items.

Reliability Statistics

Cronbach's Alpha	N of Items
.781	5

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
InterconnectednessInterdependencyLawEnforcement_6	14.30	15.593	.625	.717
InterconnectednessInterdependencyeEmergencyServices_6	14.64	14.224	.649	.706
InterconnectednessInterdependencyBankingATM_6	14.04	16.964	.497	.758
InterconnectednessInterdependencyCommunicationServices_6	14.07	17.425	.487	.761
InterconnectednessInterdependencyHealthcareServices_6	15.14	15.928	.525	.751

However, the health care services item does not tie into the overall theme of this factor and was therefore dropped.

For the three items comprising the plant operations factor, $\alpha = .467$ and the reliability would not be improved by the removal of any items. The α reliability is extremely low, which suggests that there is no real internal consistency in the measurement. However, this factor is still retained as it emerges as a relevant offender decision-making factor in the interviews as well.

Reliability Statistics

Cronbach's Alpha	N of Items
.467	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ConequenceImpactModificationSafetySettingsSystemConfigurations_3	11.80	5.201	.351	.322
ConsequenceDevastatingOperations_3	12.31	5.110	.256	.408
ConsequenceDevastatingPhysicalPlant_3	12.01	5.336	.228	.435
ConsequenceImpactDenialDisruptionService_3	11.84	5.361	.244	.418

Thus five factors were retained for the Result category, namely 'Human health'; 'Environment & health'; 'Order & finance'; 'Plant operations'; 'Information-related'.

Reactive Category

The Reactive category included survey items for the 'Response & Recovery' factor of PARE RISKS. This category had 21 items, and with a pairwise deletion the subjects varied from 259 to 283, which resulted in subject to item ratio of 12 to 13 cases respectively. For the KMO index of sampling adequacy, values above 0.6 were required for a good factor analysis. The value of 0.679 was good.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.679
Bartlett's Test of Sphericity	Approx. Chi-Square	1468.414
	df	210
	Sig.	.000

The Total Variance Explained Table below identified the initial eigenvalues and proportions of variance explained by each factor. The scree plot for the first EFA on the Reactive category had suggested that four factors were to be retained. The second EFA was therefore done with four fixed factors, which were extracted in the factor solution. Looking at the proportions of variance, the bulk of the variance attributable to the retained factors was explained by the first (general) factor (21% out of 47%) in the initial solution, whereas the variance was slightly more evenly distributed in the rotated solution (13.93%, 7.99%, 8.32%, 10.58%).

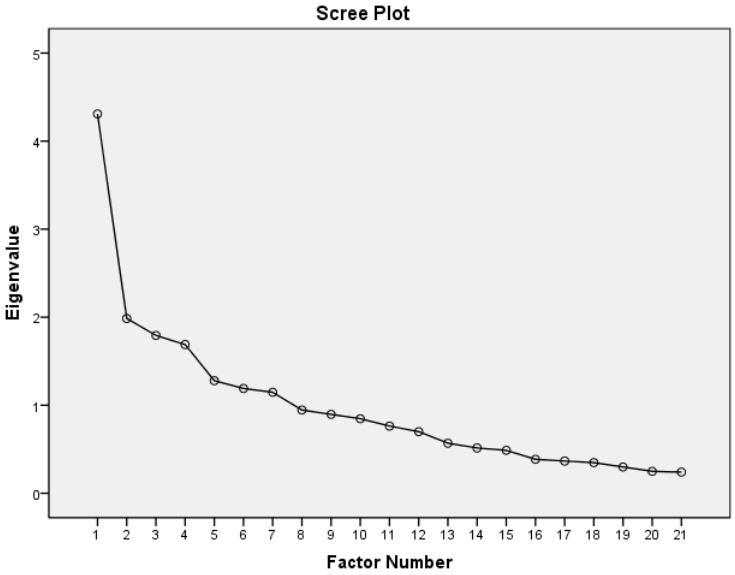
Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]	
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance
1	4.309	20.519	20.519	3.688	17.561	17.561	2.926	13.93333
2	1.986	9.456	29.975	1.379	6.567	24.128	1.677	7.985714
3	1.793	8.537	38.512	1.223	5.824	29.952	1.747	8.319048
4	1.689	8.043	46.554	1.019	4.853	34.806	2.222	10.58095
5	1.279	6.090	52.644					
6	1.190	5.669	58.313					
7	1.146	5.459	63.772					
8	.946	4.502	68.275					
9	.896	4.267	72.542					
10	.847	4.033	76.575					
11	.763	3.634	80.209					
12	.700	3.333	83.542					
13	.568	2.706	86.248					
14	.514	2.449	88.697					
15	.487	2.321	91.018					
16	.385	1.835	92.854					
17	.366	1.743	94.597					
18	.348	1.658	96.254					
19	.298	1.420	97.674					
20	.248	1.183	98.857					
21	.240	1.143	100.000					

Extraction Method: Principal Axis Factoring.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Next, the scree plot gave an indication of how many factors were to be retained. The change in slope, or the 'elbow' was a useful guide. In the plot below, this discontinuity occurred at four factors, and so a four-factor solution was considered.



In order to determine what these factors were, the pattern matrix was analyzed next. The *first* factor was readily interpretable as international reaction and had six items, with loadings of detection by secret service (.658), detection by CIA (.667), detection by military (.541), response by secret service (.536), response by CIA (.599), and response by military (.454). The *second* factor was readily interpretable private-public reaction and had four items, with loadings of private security firm detection (.461), police department detection (.614), private security firm response (.531), and police department response (.632).

The *third* factor was readily interpretable as national reaction and had three items, with high loadings of FBI detection (-.711), FBI response (-.517), and DHS detection (-.450). Another item also loaded onto this factor; however not only did it not fit with the national reaction theme, but it also had the opposite signatory value compared to the other items that loaded onto this factor: private security firm response (.381). Hence this item was dropped.

The fourth factor was not readily interpretable as it had six items which did not tie together logically [industry detection (.544), FCC response (.505), CERT detection (.501), industry diffusion (.460), FCC detection (.442), and CERT response (.402)]. As such, this factor was dropped

This solution did not have factor purity, as some items did not load highly on just one factor, and so the factors were not clearly defined by the groupings of tests that load on them. Additionally, only one factor (international reaction) had 5 or more strongly loaded items (.50 or better), which was desirable and indicative of a solid factor (Costello & Osborne 2005).

Pattern Matrix[a]

	Factor			
	1	2	3	4
WorryCIA_5	.667			
WorrySecretService_5	.658			
RespondCIA_5	.599			
WorryMilitary_5	.541			
RespondSecretService_5	.536			
RespondMilitary_5	.454			
RespondPoliceDepartment_5		.632		
WorryPoliceDepartment_5		.614		
RespondPrivateSecurityFirms_5		.531	.381	
WorryPrivateSecurityFirms_5		.461		
WorryFBI_5			-.711	
RespondFBI_5			-.517	
WorryDHS_5			-.450	
RespondDHS_5				
DetectionResponse_5				.544
RespondFCC_5				.505
WorryCERT_5				.501
DiffusionResponse_5				.460
WorryFCC_5				.442
RespondCERT_5				.402
RestorationPeriod_5				

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.
a. Rotation converged in 12 iterations.

It is worth knowing whether a scale defined by factor loadings is really measuring a unitary construct. The usual index of the internal consistency of a scale is, as noted above, Cronbach's α. As noted earlier, a value between .7 and .8 is an acceptable value for Cronbach's α, although a lenient cut-off of .60 is common in EFA (Field 2005).

For the six items comprising the international reaction factor, α = .765 and the reliability would not be improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.765	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
WorryCIA_5	15.79	25.097	.566	.716
WorrySecretService_5	15.47	25.119	.552	.719
WorryMilitary_5	15.51	25.574	.514	.729
RespondCIA_5	15.01	25.123	.485	.738
RespondSecretService_5	14.82	25.887	.490	.736
RespondMilitary_5	14.53	26.768	.444	.747

For the two items comprising the private-public reaction factor, $\alpha = .651$ and the reliability would obviously not be improved by removal of any of the items.

Reliability Statistics

Cronbach's Alpha	N of Items
.651	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
WorryPoliceDepartment_5	10.53	9.258	.464	.564
WorryPrivateSecurityFirms_5	10.21	9.323	.437	.581
RespondPoliceDepartment_5	11.03	7.903	.450	.574
RespondPrivateSecurityFirms_5	10.40	9.241	.387	.613

For the three items comprising the national reaction factor, $\alpha = .628$ and the reliability would be slightly improved by removal of the DHS detection item (.656).

Reliability Statistics

Cronbach's Alpha	N of Items
.628	3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
WorryFBI_5	4.05	3.362	.562	.355
WorryDHS_5	3.40	3.157	.376	.656
RespondFBI_5	4.25	4.225	.411	.572

Thus three factors were retained for the Reactive category, namely ‘International’; ‘National’; and ‘Public-private’.

Aunshul Rege

Date and Place of Birth: November 13, 1979, India

Education	**Dates**
Richmond High, Richmond, BC, Canada	11/1994-05/1997
University of British Columbia, Vancouver, BC, Canada -BSc Computer Science	09/1997-05/2002
Saint Mary's University, Halifax, NS, Canada -BA (Hons.) Criminology	09/2004-05/2006
Saint Mary's University, Halifax, NS, Canada -MA Criminology	09/2006-05/2008
Rutgers University, Newark, NJ, USA -MA Criminal Justice	09/2008-05/2010
Rutgers University, Newark, NJ, USA -PhD Criminal Justice	09/2010-05/2012

Employment	**Dates**
Software Engineer, Canadian Securities Registration Systems, Burnaby, BC, Canada	11/2002-03/2004
Programmer/Researcher, Campus Security, Saint Mary's University, Halifax, NS, Canada	09/2005-09/2006
Research Assistant, Nova Scotia Gaming Corporation funded 'Commercial Advertising & Adolescent Gambling Project', Halifax, NS, Canada	01/2007-07/2007
Teaching Assistant, Rutgers School of Criminal Justice, Newark, NJ, USA	09/2010-05/2011
Teaching Assistant, Rutgers School of Criminal Justice, Newark, NJ, USA	09/2011-05/2012

Publications

-Rege, A. (2011). Digital Information Warfare Trends in Eurasia. Security Journal, conditionally accepted.

-McMullan, J. & Rege, A. (2010). Online crime and internet gambling. Journal of Gambling Issues. Issue 24, July 2010.

-Rege, A. (2009). What's Love Got to Do With It? Exploring Online Dating Scams and Identity Fraud. International Journal of Cybercriminology, 3 (2).

-Rege-Patwardhan, A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. Criminal Justice Studies, 22 (3).

-McMullan, J. & Rege, A. (2007). Cyber-Extortion at Online Gambling Sites: Criminal Organization and Legal Challenges. Gaming Law Review, 11 (6).