Securing Oil and Natural Gas Infrastructures In the New Economy

National Petroleum Council

June 2001

Securing Oil and Natural Gas Infrastructures In the New Economy

A report by the
National Petroleum Council

Committee on Critical Infrastructure Protection
David J. Lesar, Chair

June 2001

NATIONAL PETROLEUM COUNCIL

Archie W. Dunham, *Chair*
William A. Wise, *Vice Chair*
Marshall W. Nichols, *Executive Director*

U.S. DEPARTMENT OF ENERGY

Spencer Abraham, *Secretary*

The National Petroleum Council is a federal advisory committee to the Secretary of Energy.

The sole purpose of the National Petroleum Council is to advise, inform, and make recommendations to the Secretary of Energy on any matter requested by the Secretary relating to oil and natural gas or to the oil and gas industries.

Library of Congress Catalog Card Number: 2001091810

Printed in the United States of America

Table of Contents

Executive Summary

INTRODUCTION

Based on the finding of a growing potential vulnerability, the President of the United States issued, in May 1998, a directive outlining the Administration's policy on critical infrastructure protection. An accompanying White Paper to the directive states:

> Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Study Request

In response to the President's policy directive, the Secretary of Energy requested the National Petroleum Council's (NPC's) advice "on cooperative approaches to protecting the critical infrastructure of the United States oil and gas industry."

In his April 7, 1999 letter, the Secretary specifically asked the Council to:

- Review the potential vulnerabilities of the oil and gas industries to attack, both physical and cyber
- Provide advice on policies and practices that industry and government, separately and in partnership, should adopt to protect or recover from such attacks.

(See Appendix A for the full text of the Secretary's request letter and a description of the National Petroleum Council.)

Study Organization

The NPC established the Committee on Critical Infrastructure Protection to respond to the Secretary's request. The Committee was chaired by Richard B. Cheney, Chairman of the Board and Chief Executive Officer, Halliburton Company, until August 16, 2000. He was replaced by David J. Lesar, Chairman of the Board, President, and Chief Executive Officer, Halliburton Company. Eugene E. Habiger, then Director of the Office of Security and Emergency Operations, U.S. Department of Energy, served as the Committee's Government Cochair. A Coordinating Subcommittee was formed to assist the Committee in conducting the study and preparing a draft report for the NPC's consideration. This Subcommittee was chaired by Charles E. Dominy, Vice President, Government Affairs, Halliburton Company. Paula L. Scalingi, Director of the Office of Critical Infrastructure

Protection, U.S. Department of Energy, served as the Subcommittee's Government Cochair. (See Appendix B for rosters of the Committee and Coordinating Subcommittee.)

Background

Over the past decade, the world has been changed by the information technology and telecommunications (cyber) revolution. As a result of these changes, global institutions have become more effective and productive.

Because of the pervasive use of cyber systems, they have become an interwoven part of the critical infrastructures. The United States, as does the rest of the world, faces an increasing number of threats to its infrastructures that are essential in times of peace and war. The threats faced are not only the traditional ones of natural disasters, human error, and attacks on physical assets, but now include threats to the cyber systems upon which today's economy is so dependent.

In the past, the oil and natural gas industries have effectively protected physical facilities. The protection of cyber systems has not kept pace with companies' ever-increasing dependence on them. The oil and natural gas industries have undertaken this study to better understand potential vulnerabilities and study methods for mitigating them.

Among the initiatives undertaken by the federal government related to infrastructure protection, two form the basis of the request for this study: the President's Commission on Critical Infrastructure Protection and Presidential Decision Directive 63. Undoubtedly, there will be more efforts in this area as the use of cyber-based systems expands globally.

The President's Commission

In July 1996, the President of the United States established the President's Commission on Critical Infrastructure Protection. The Commission's purpose was to assess the vulnerabilities of existing infrastructures and to recommend a comprehensive national policy and implementation strategy for protecting our nation's critical infrastructures. In its October 1997 report, *Critical Foundations: Protecting America's Infrastructures,* the Commission identified eight critical infrastructures that are considered to be so vital that their incapacity or destruction would have a debilitating effect on our defense and economic security. These infrastructures are information and communications (telecommunications), banking and finance, water supply, electric power, oil and natural gas, transportation, government services, and emergency services (including medical, police, fire, and rescue).

Since many of these critical infrastructures are owned and operated by the private sector, as is the case for the oil and natural gas infrastructure, it is essential that the government and private sector work together. This theme of partnership in addressing critical infrastructure protection needs was embraced by the Commission and emphasized in its final report, *Critical Foundations*.

Presidential Decision Directive 63

In May 1998, President Clinton issued Presidential Decision Directive 63, *Protecting America's Critical Infrastructures,* which built on the recommendations of the President's Commission that called for a national effort to ensure the security of the nation's critical infrastructures. The goal of the decision directive was that critical infrastructure protection programs would reach "initial" operating capability in the year 2000, and full capability no later than 2003.

The directive provided a framework for working with the identified critical infrastructure sectors to develop individual plans and meet the directive's goals. Each sector would be led by their governmental regulatory department or agency. The "lead agency" would appoint a "sector coordinator" to work with each of their sectors.

The energy sector's lead agency is the Department of Energy. The Department of Energy asked the North American Electric Reliability Council to be the electric power sector coordinator. As an interim measure, the National Petroleum Council was asked to be the sector coordinator for the oil and natural gas industries. At the request of the Department of Transportation, oil and gas pipelines were added to the area being addressed by the National Petroleum Council. As outlined in this study, others in the oil and gas industries will assume the role of sector coordinator when this study is forwarded to the Secretary of Energy.

Status of Federal Critical Infrastructure Protection Activities

In February 2001, President Bush submitted to Congress a report on the status of federal critical infrastructure protection activities.[1] The report also reviewed government and industry progress toward the objectives outlined in Presidential Decision Directive 63.

Study Report

This NPC report suggests actions for identifying and reducing infrastructure vulnerabilities within the oil and natural gas industry sector. It raises the level of awareness and understanding of these new critical infrastructure protection challenges within our industry and government. It presents the business case for moving forward in this new business environment, adopting critical infrastructure protection thinking as part of the foundation of acting in the best interests of a company. It identifies the issues and the steps forward that the oil and natural gas industries and the government will need to implement, in partnership, to ensure the integrity and continuity of the industries' infrastructure.

This report's recommendations are intended to be dynamic, reflecting the fact that the industry is in the midst of significant change. Even the understanding of critical infrastructure protection is still evolving. While the Secretary's letter specifically mentioned attacks, the scope of the study has expanded beyond that to include many potential disruptions and vulnerabilities. Energy infrastructures are inextricably linked with other critical infrastructures, and, as a result, a holistic perspective on critical infrastructure protection is essential.

The National Petroleum Council recognizes that some of the issues addressed in this report must be explored in greater depth and that some of the recommendations may warrant follow-on investigation. It is the intent of the NPC that this report will provide a basis for constructive debate and serve as a foundation for the next steps in developing a viable blueprint for the energy industry and the nation.

FINDINGS

New Business Environment and Critical Supporting Infrastructures

Society has moved from a model of gradual change to one of exponential change because of development and reliance on cyber and other electronic systems. Such change is pervasive, throughout every aspect of business, government, and personal lives. Advances are expected to continue at an exponential rate, affording no return to the traditional model. Significant advances in information technology (IT) and telecommunications are enabling the change to a new, interconnected, global economy. With these advances, the nature of security issues is expanding to include threats and vulnerabilities associated with cyber and other electronic systems. The new economy is supported by and increasingly dependent on several critical infrastructures as identified by the President's Commission on Critical Infrastructure Protection:

- Oil and natural gas
- Electric power

[1] http://www.ciao.gov/CIAO_Document_Library/CIP_2001_CongRept.pdf.

- Information and communications (telecommunications)
- Transportation
- Banking and finance
- Water supply
- Government services
- Emergency services (including medical, police, fire, and rescue).

Oil and Natural Gas Industries in the New Economy

The oil and natural gas industries provide almost 62% of the energy used in the United States. These energy sources are vital and directly underpin much of the U.S. economy. The oil and natural gas industries are experiencing the same exponential changes as the rest of the economy. While this sector's physical footprint appears the same—wells, gathering systems, processing facilities, transmission systems, and distribution systems—the approach to operating the industries, both from a physical and business perspective, has changed. Many of the changes are directly linked to the burgeoning use of electronic communications and have resulted in modifications such as the use of advanced electronic control systems and business arrangements based on electronic transactions. For example, systems that control operating processes within refineries, along pipelines, and in producing fields were previously closed and proprietary. These control processes are now moving toward open architecture and commercially available software. Also, much of the raw material and product that is purchased and sold is accomplished using electronic-based futures markets. Because of the alterations in equipment configuration and corporate re-engineering, many of the changes are essentially irreversible.

Today, organizational changes such as mergers, alliances, and joint ventures have resulted in organizations that no longer resemble the energy companies of the past. These changes have resulted in the transformation of service companies, and blurred the lines between traditional oil, natural gas, power, and pipeline companies.

New Electronic and Interconnected Economy

Information is becoming universally and instantaneously available. This is leading to a strong global business network available to all regardless of size, financial strength, or purpose. The growth in the availability and dependence on electronic systems, due to the expectation of synergy, has created a marked increase in the interdependence of entities. Information is more transparent, difficult to protect, and easily transferred. These electronic systems are interconnected globally, making traditional physical boundaries less important.

The critical infrastructures outlined by Presidential Decision Directive 63, including those of the oil and natural gas industries, have a common dependency on IT and telecommunication systems. Additionally, electric power and water supply systems use supervisory control and data acquisition (SCADA) operating systems similar to those used by the oil and natural gas industries. As time passes, an increasing amount of information is available in an electronic format. Consequently, information is subject to either accidental or deliberate corruption, theft, or denial of access. Organizations have to deal with the challenge of information assurance as a condition of doing business in today's world.

Vulnerabilities, Consequences, and Threats

The introduction of cyber technologies has increased risks in the oil and natural gas industries. The traditional security approach has been to physically protect personnel and property from human error or natural disasters. Emergency plans to deal with such events remain in place. However, processes are inadequate to deal with the changes that are accompanying the increased dependence on cyber and other elec-

tronic systems. This critical reliance is a recent phenomenon resulting in new threats and a high level of vulnerability because the development and adoption of processes to ensure security in this area has not kept pace. The new weapon is electronic bits, versus bombs in the old paradigm.

In this new paradigm, individuals and groups, from hackers to organized terrorists, have the ability to simultaneously attack multiple sites. Because the success of such attacks are often disseminated to a wide audience, they often become the blueprint for additional attacks. Beyond cyber attacks, human error and normal system failures continue, which because of the growing level of interconnectivity of systems, have the capability of doing far more damage than in the past. The consequences of these attacks and failures are more difficult to predict, and potentially more extensive.

The reliance on cyber technologies creates the opportunity for interrupted communications, false or misleading transactions, fraud, or breach of contracts, and can result in potential loss of service, loss of stakeholder confidence, or the failure of the business itself. The due diligence standards in this new environment remain ill defined and transitory. Also, when infrastructure disruptions occur, conflicts of interest can develop between the various entities involved, that inhibit response, restoration of service, and future infrastructure protection.

Risk Management and Vulnerability Mitigation

In addressing risk management and vulnerability mitigation, the study concluded that companies in the oil and natural gas industries will benefit from conducting periodic vulnerability assessments of their own systems and operations, both physical and electronic. In many situations, the global nature of doing business today has resulted in an intertwining of cyber systems between organizations. Therefore, assessments of partners' vulnerabilities, with joint vulnerability mitigation efforts, may be important to protect business relationships. The vulnerability of interdependencies with other infrastructures should also be an inherent part of these assessments.

Response and Recovery

Most companies understand and are able to handle their own physical infrastructure disruptions. Cyber response and recovery capabilities and processes are not as mature as those developed to handle physical incidents. Increased use of automation, increased interconnectedness, just-in-time business models, and interdependencies can potentially result in regional, national, or international incidents and impacts. The increasing use of information and communications technology and the potential for these broader consequences are generating new challenges for response and recovery planning.

These increasingly complex response and recovery environments dictate that plans be periodically tested to ensure they will manage emergencies and reduce risk for all stakeholders. This new business environment dictates that companies include key stakeholders, such as business partners, suppliers, customers, and representatives from local and state governments in response and recovery tests and exercises.

When infrastructure disruptions occur, the roles and responsibilities of local, state, and federal governments often conflict. These conflicts of interest regarding jurisdiction impede timely restoration of service and can also inhibit timely development of infrastructure protection processes. Timely and actionable information is important for effective response to threats or incidents, as well as for successful recovery actions. Companies can benefit by having an effective internal information-sharing mechanism to receive, analyze, and disseminate incident information to enhance response and recovery.

Information Sharing and Sector Coordination

In the oil and natural gas industries, only limited capabilities exist for sharing information on physical and cyber incidents, threat assessments, and vulnerabilities. Receipt of real-time information is critical in protecting the oil and natural gas infrastructures, and rapid reporting of incidents is vital. A broader base of participation in information sharing enhances the timely flow of information. Sharing of information, however, raises uncertainty concerning liability, privacy, and antitrust issues. Centralized collection of specific vulnerability data could create a source of information that could be used for nefarious purposes. Under current law, there is uncertainty about the government's ability to keep information from public release. Such a release could result in loss of investor confidence, shareholder value, and business reputation.

This study concludes that information sharing related to threats and responses to threats would be beneficial to the oil and natural gas sector. Of the three general models for implementing an information sharing mechanism (reliance on industry staff, use of an industry-directed service provider, or a hybrid government/industry management), the industry-directed service provider model is the most efficient and appropriate for the oil and natural gas sector.

A permanent sector coordinator should be designated to lead the critical infrastructure information sharing effort and to be the focal contact point for other oil and natural gas industries critical infrastructure issues.

Legal and Regulatory Uncertainties in the New Economy

There are many legal uncertainties regarding the electronic aspects of the new economy. While laws and legal procedures are emerging, they have yet to be tested by the judicial process in any significant way. International law, where it exists, often varies from U.S. law and is either more or less stringent, or conflicting. Risks associated with cyber and other electronic systems often involve intangible, highly uncertain potential losses.

Corporate structures are changing, with mergers, joint ventures, alliances, and increased dependence on outsourcing. Consequently, the oil and natural gas industries have become more reliant on contract law. A variety of efficiency moves are now commonplace and often involve non-U.S. entities making national differences in legal approach an added complexity. There has been a shift of the energy enterprise among providers, marketers, and systems. These accelerated changes in ownership along with changes in industry roles and responsibilities are occurring throughout the industry. Business restructuring is moving from the traditional "wires" and "pipes" business to non-traditional investments (e-business activities). All of these changes impact the robustness of the oil and natural gas infrastructure.

Research and Development

When considering critical infrastructure protection research and development (R&D) in areas such as information technology, the oil and natural gas industries do not have unique expertise, and primarily rely on commercial providers to conduct the necessary R&D. The government conducts a broad range of R&D activities in this area, the results of which could be used to meet infrastructure protection, mitigation, and response and recovery needs by the oil and natural gas industries. This includes R&D on information assurance and other national security areas. The government should assure through consultation with industry that R&D pursued reflects industry and government needs, and is not redundant with private-sector efforts. There needs to be an effective method for providing greater technology transfer to industry, particularly from its national defense and other classified research programs.

The Successful Y2K Model

The Y2K experience provides a good "go forward" model for government and industry. It emphasized the risks faced by the government and private sectors due to the interconnectivity and interdependency of their respective critical infrastructures. Y2K also demonstrated that significant challenges to national interests could be addressed through information exchange, the removal of legal barriers, and elimination of the fear of federal, state, and local government intervention.

RECOMMENDATIONS

Based on the findings of this study, the National Petroleum Council recommends that industry and government take the following specific actions to better protect the critical infrastructures of the oil and natural gas industries. The business case for taking proactive measures is persuasive and instructive. The energy industry cannot do this alone. The challenges of the new economy and the increasing interdependencies among and within our infrastructures necessitate that industry must work with other sectors, and with federal, state, and local governments.

Vulnerability Assessments, Information Assurance Process, and Planning Recommendations

- **Vulnerability/Risk Management Assessments.** Each company should regularly conduct vulnerability assessments of its own systems and operations and take action as appropriate. In addition, each company should conduct assessments of its partners' vulnerabilities. Risk management processes should be reviewed to ensure that both electronic and physical security is included.

- **Information Assurance Process.** Industry and government should advocate the development, adoption, and implementation of global IT management processes to reduce vulnerabilities of the cyber and other electronic systems on which the oil and natural gas industries are dependent. A good example of such a process is the International Standards Organization (ISO) 17799, "The Standard for Information Security Management."

- **Response and Recovery Planning.** The oil and natural gas industries should enhance their response and recovery plans as they relate to information technology system disruptions, while continuing their traditional role of maintaining and implementing plans for disruptions to physical facilities. Individual companies should consider engaging in regional response and recovery planning and exercises to deal with disruptions to physical and cyber infrastructures resulting from natural disaster, system failure, human error, or sabotage. Additionally, industry must take into account the challenges of the new business environment, including infrastructure interdependencies, and enhance response plans to ensure they are adequate and coordinated with other infrastructures, regional, state and local emergency response programs.

Information Sharing and Sector Coordination Recommendations

- **Information-Sharing Mechanism.** The oil and natural gas industries should establish a secure information-sharing mechanism to collect, assess, and share with its members information on physical and electronic threats, certain vulnerabilities, incidents, and solutions/best practices. This mechanism also would gather and receive information from government, technology providers, and other information sharing mechanisms. The specific type of mechanism recommended is commonly called an information sharing and analysis center (ISAC). Of the three general models for ISACs, the industry-directed service provider model is the most efficient and appropriate for the oil and natural gas sector. Under this model, the

oil and natural gas industries' ISAC would likely be a non-profit, cooperative organization.

- **ISAC Membership.** Under the current law and legal environment, the ISAC would only share information within the oil and natural gas industries. Therefore, membership would be initially restricted to private-sector companies operating in the oil and natural gas industries. Consideration should be given to allowing industry associations to join in order to disseminate information to smaller oil and natural gas companies. Private companies who share similar technologies, such as the electric and water supply industries, may be encouraged to join at a later time. Eventually this may be extended to other entities, as interrelationships become apparent.

- **Implementation.** The oil and natural gas industries will take the lead in establishing a board, which will investigate, develop, and implement an ISAC for the sector.

- **Sector Coordination.** While no organization represents all segments of the oil and natural gas industries, it is recommended that the Secretary of Energy formally acknowledge the designee of the governing body of the oil and natural gas industries ISAC as the sector coordinator.

Government Action Recommendations

- **Legislative Actions.** The federal government should enact legislation to facilitate information sharing with and among sector components. Communications with government involving critical infrastructure protection information should be exempted from the provisions of the Freedom of Information Act. Also, legislation should be enacted to provide liability and antitrust relief for critical infrastructure protection information sharing similar to the law covering Y2K activities. While the need for individual privacy is recognized, the need must be balanced against the critical nature of protecting infrastructures as regulations are formulated and laws are enacted.

- **Access to Law Enforcement and Intelligence Information.** The industry would benefit from real-time, relevant vulnerability and threat information that is only available to government under current conditions. Government and industry should work together to develop processes that ensure the sharing of relevant information.

- **International Initiatives.** The federal government should use all means available to encourage countries to enact globally consistent laws addressing the interconnected, electronic commercial marketplace. The government could use the same approach to encourage the development and adoption of global technical standards and uniform business practices to reduce the vulnerabilities of cyber and other electronic systems. The government should undertake collaborative efforts with other nations to enhance global infrastructure assurance.

- **Holistic Approach to Energy Critical Infrastructure.** All components of U.S. energy sectors should be viewed as a single energy infrastructure in the implementation of critical infrastructure protection. U.S. energy components (i.e., oil, natural gas, electric power, other energy sources, and their transportation modes) are converging with each other in the marketplace.

- **Response and Recovery Activities.** Federal, state, and local governments should ensure coordination of response and recovery activities for significant disruptions that require actions beyond the capabilities or purview of individual companies in the oil and natural gas sector. Preplanning should be undertaken to minimize jurisdictional conflicts among government entities during the response to and recovery from a major emergency.

- **Research and Development Activities.** Government-funded research and development should address national security and other key critical infrastructure protection, mitigation, response, and recovery needs that transcend individual companies in the oil and natural gas sector, with other areas being the focus of R&D by commercial technology providers. The federal government should work with industry to focus and prioritize its funding of critical infrastructure protection research and development. Government should also provide for the rapid transfer to the private sector of government-funded R&D applicable to critical infrastructure protection, especially in the information technology and telecommunications areas.

- **Continued Support for Critical Infrastructure Protection Initiatives.** The government should continue its critical infrastructure protection initiatives, working closely with the oil and natural gas industries and other critical infrastructures to protect the country's national security, economic health, and social well being. The government should be organized to effectively interact with industry on a broad range of mutual critical infrastructure protection issues.

CHAPTER 1

The New Business Environment

Most of the understanding of the oil and natural gas business is founded on what can be viewed as the "old business environment." This environment evolved over a century during which there were many significant social, economic, and technological changes that shaped the world in which the oil and natural gas business existed. Over the past decade, there have been many changes in U.S. business structure that have caused significant shifts in the way in which business is done. These changes have been so great that a "new business environment" has emerged.

The oil and natural gas industries find themselves in a world that is more complex due to unprecedented social and technological change in timeframes that were unimaginable a decade ago. In order to compete in the new business environment, it has been necessary for the oil and natural gas industries to place a critical reliance on electronic infrastructure. The industries have long been able to adequately protect their physical infrastructures. However, the addition of the electronic infrastructure to the mix has resulted in new concerns regarding physical infrastructure protection as well as for protection of the electronic infrastructure itself. Electronic tools have been developed at a rapid rate and have been quickly incorporated by the oil and natural gas industries in their electronic infrastructure. The pace at which these changes have taken place has been so fast that adequate measures for critical infrastructure protection have lagged behind. A holistic approach to security that includes cooperation between the private and public sectors is necessary if exposure to unacceptable risk is to be avoided in the new business environment.

U.S. BUSINESS STRUCTURE

Today the business community in the United States is composed of a mix of differing structures. At one extreme there are the "old business" models where capital investment and slow change is a major component. At the other end is the "new business" model where rapid deployment of information and globalization are the primary operating factors. Typically the oil and natural gas companies were representative of the "old business" model, while the "new business" model was perceived as the companies in the e-business driven digital economy. While it was convenient to think in this stratified manner, there are few organizations that are either one or the other. In most cases, organizations that exist today are rapidly employing the information techniques that typify the "new business" model companies.

Today the U.S. business system has entered what can be thought of as the new business environment.

- Today's business environment is markedly different from experiences of the past because of the rapidity at which change takes place.
- A distinguishing feature is the increase in the formation of new business organizations ranging from mergers to joint ventures and, often, new entrants into businesses through acquisition of facilities.
- Organizations have expanded in geographical scope, often moving from local or regional to national or global in nature.
- Operations have increasingly become automated, not only on at specific sites, but at

remote locations, allowing operations for a widely dispersed organization to be controlled from one location.

- Advances in information technology and telecommunications have permeated all aspects of the new business environment resulting in creative business models, i.e., business to business, business to consumers, and electronics commodity trading.

These factors when combined with rapidity of communication and transparency of marketplace fundamentals have led to reducing the workforce size, changing the skill characteristics required in the workforce, just-in-time focus in operations, and a significant increase in the interdependence of organizations.

While business has been a major recipient of change, the customer and governments have not been left out. The customer expects to be the ultimate recipient of the benefits of the new mode of doing business. Conversely, the customer does not expect to be inconvenienced by the disruptions that might occur as a result of the new business environment. Governments have become confused by jurisdictional conflicts in that what was once clearly local may now be national or international. The instant availability of information has encouraged experiments with price decontrol in businesses that were once heavily regulated. All of these changes leave government entities, customers, and companies confused as to what their roles are in the new business environment.

THE OIL AND NATURAL GAS INDUSTRIES

While all of the foregoing are important and each of the individual areas could be the subject of an in-depth study, this National Petroleum Council study effort is targeted at the security of infrastructure in the oil and natural gas sector. For the past decade, the social and economic foundations upon which understanding and system development in the oil and natural gas industries are predicated have been assaulted by an emerging technology: electronic information integration and exchange.

This technology is changing the way in which oil and natural gas companies do business. Primarily the change relates to instant availability of information, transparency of data, and the speed at which communications take place. Many of the changes that have taken place in the past were driven by major events or inventions, most of which took many years to permeate the business fabric of the nation and the world. Information technology and the communication revolution it creates have taken the world of business by storm in a very global way. National boundaries, which used to provide some stability for business activities, no longer are a limitation. Information, which used to be relatively easy to protect physically, is potentially vulnerable to an individual who has access to a computer and a way into the global information network.

These issues have rapidly become factors reshaping the business landscape, arriving at such a rapid pace that the business community's traditional method of accepting change has been overwhelmed. The slower traditional evolutionary pace that has provided security measures to deal with change in the past is today unable to effectively cope. Widespread, creative understanding and action are needed in the oil and natural gas business sector to provide for a secure infrastructure environment, allowing for stable and relatively consistent approaches to the conduct of business in the future.

The factors that are driving the oil and natural gas new business environment are technology, globalization, organization, and legal and regulatory issues.

Technology

Yesterday most technology was focused on the operational functions of finding, producing, trans-

porting, refining/manufacturing, and selling oil and natural gas and their products. Today's technology, as epitomized by rapid electronic data collection, electronic data transfer, and Internet communication, has been transformational. It has made the "impossible" possible, it impacts every aspect of the oil and natural gas business, and it has added a whole new set of players. Many companies have transformed their business focus from one of ownership of physical assets to one of intellectual and information value added. Ubiquitous networks and systems that seamlessly cross functional, organizational, and geographical boundaries enable this new model. Automation has driven down costs and reduced human intervention in many traditional processes. The drive for global systems in the procurement or supply chain management segment of the business has lowered the barriers for participation by suppliers, agents, distributors, and even consumers, and has brought together alliances of financial services, traders, oil and natural gas producers, and governments.

Consequently, we simply can't turn back the clock. The people, skills, and physical structures of the old business environment no longer exist and cannot be reconstructed under today's conditions. Today the exposure to cyber incidents is greater and the consequences are potentially more devastating than when physical infrastructure was the only concern. Interdependencies have been created that heighten the risk of intrusion and increase exposure. Essentially, anyone with a laptop, modem, and phone line or wireless electronic interface has the potential to cause billions of dollars worth of damage. Incident response is more complex and broader reaching than ever before and the time to recover is longer.

Globalization

Yesterday we had regional and local markets. Communication was relatively slow, access to information was limited, and markets were slow to change. Today markets are global in nature as countries are being forced by pressure from worldwide competition to open their markets. With almost instantaneous access to information, markets are also more transparent and efficient, and, therefore, highly competitive.

As a consequence, companies continuously face cost-reduction pressure in the new marketplace. In order to participate in today's marketplace, many oil and natural gas companies must move from a local to a global perspective, which often requires formation of globalized, strategic partnerships to have sufficient reach. All of these factors require full reliance on an electronic infrastructure.

Global competitiveness has resulted in foreign ownership of former U.S. oil and natural gas infrastructures by non-U.S. companies and governments, creating additional vulnerabilities to the U.S. economy.

Organization

Yesterday the oil and natural gas industries were relatively stable, composed of large multinational companies and smaller niche players such as independents. The workforce was long serving, loyal, highly experienced "old hands" who perceived that they had a "social" contract for employment resulting in a family model. Today mega-mergers, alliances, and joint ventures have resulted in organizations that no longer resemble those of the past. These changes, encouraged by electronic information technology, have given rise to the virtual organization, resulted in significant manpower downsizing, proliferated the number of global organizations, resulted in the transformation of service companies, and blurred the lines between traditional oil, natural gas, and power companies. As a result, the work environment has become less stable, pressures build to do more with less, knowledge and experience have been "outsourced," and the "social" employment contract has been broken.

Consequently, the workforce is less loyal to a specific organization than it was in the past. Which, along with the loss of institutional knowledge, has created the potential for less experienced or disgruntled employees, either unintentionally or intentionally, to disrupt critical infrastructure. Interdependencies and electronic information flow create the potential for these disruptions to be significant, and have lessened the capability for dealing with crises in a timely fashion. Dependencies and interdependencies that did not previously exist have been created, adding complexity and additional exposures to infrastructure.

Legal and Regulatory Issues

Yesterday the law was able to focus on discreet elements of the oil and natural gas business, the players were well defined, and a century of experience had clearly set the rules. Today the law is far behind the changes wrought by the new business environment. Additionally, the advent of organizations like the European Union (EU) and the North American Free Trade Alliance (NAFTA) have brought together regulatory and legal oversight on a broader, more complex basis. Environmental regulation is now a global issue. Participation by foreign governments in ownership of former U.S. corporations, such as PDVSA ownership of CITGO or Saudi Aramco's participation in Motiva, raise such issues as sovereignty, taxing regimes, and contract law. New areas of legal and regulatory concerns are created almost daily, i.e., the author of the "ILoveYou" virus could not be prosecuted under Philippine law. Although this is not totally unprecedented, it is the speed at which these changes occur that is the ultimate concern.

As a consequence, the tendency of regulators and lawmakers may be to "slow up" the process. The result is likely to be the creation of laws and regulations that cause conflict at local, state, national, and international levels simply due to the newness and complexity of the situation. The lack of certainty and increased ambiguity may result in more exposure of electronic systems to exploitation by either unintentional or willful intrusion.

FINDINGS AND CONCLUSIONS

- Society has moved from a model of gradual change to one in which change takes place at a rate that was unimaginable in the past.
- Markets and organizations serving these markets are increasingly becoming more global in nature and complex in structure, all possible because of the intense use of electronic communications and information technology.
- To remain competitive, industry participants are becoming more dependent on electronic systems. Therefore, the rapidity with which change occurs is expected to continue and is likely to increase in the future.
- Changes are occurring in the oil and natural gas industries because of the ever-increasing use of electronic communications and information technology exacerbated by globalization.
- As a result of the move to more complex structures and lower levels of staffing, workforces have become less loyal to a specific organization and less steeped in institutional knowledge. This combined with the high level of interconnection in the marketplace provides for the opportunity of major disruptions when an employee, either unintentionally or intentionally, interrupts the flow of electronic information.
- As the new business environment intensifies, the return to older more traditional methods of conducting business becomes more difficult, if not impossible. Therefore, there is no "turning back."

- The legal aspects of doing business in the new business environment are shifting from the premise that there were discrete elements of the oil and natural gas industries around which bodies of law were focused to a condition where there is a high degree of interconnection between business segments, companies, and nations. Because of the rapidity of this shift in structure, the law has been slow to adapt and is far behind today's needs.

CHAPTER 2

Vulnerabilities, Consequences, & Threats

The oil and natural gas industries are continuously changing. These large well-developed infrastructures were physically separate businesses, composed of the following:

- **Physical Infrastructure.** The oil and natural gas infrastructures relied on their physical components and individual isolated systems.
- **Human Capital.** The oil and natural gas infrastructures relied on a loyal dedicated staff to operate, maintain, and restore service. Computers have been used by these infrastructures for a long time, but the heart of the physical operation of these infrastructures was manual.
- **Stable Business Environment.** The oil and natural gas infrastructures operated in a relatively stable business environment. The industry participants, regulations, and technology all remained fairly consistent.

Figure 2-1 portrays a historical integrated oil and natural gas model. These infrastructures obtain raw feedstocks throughout the world, move them through "manufacturing" to create products, and then move them to market. Figure 2-1 also notes that these industries rely on other infrastructures.

As discussed in Chapter 1, the rapid proliferation and integration of information technology

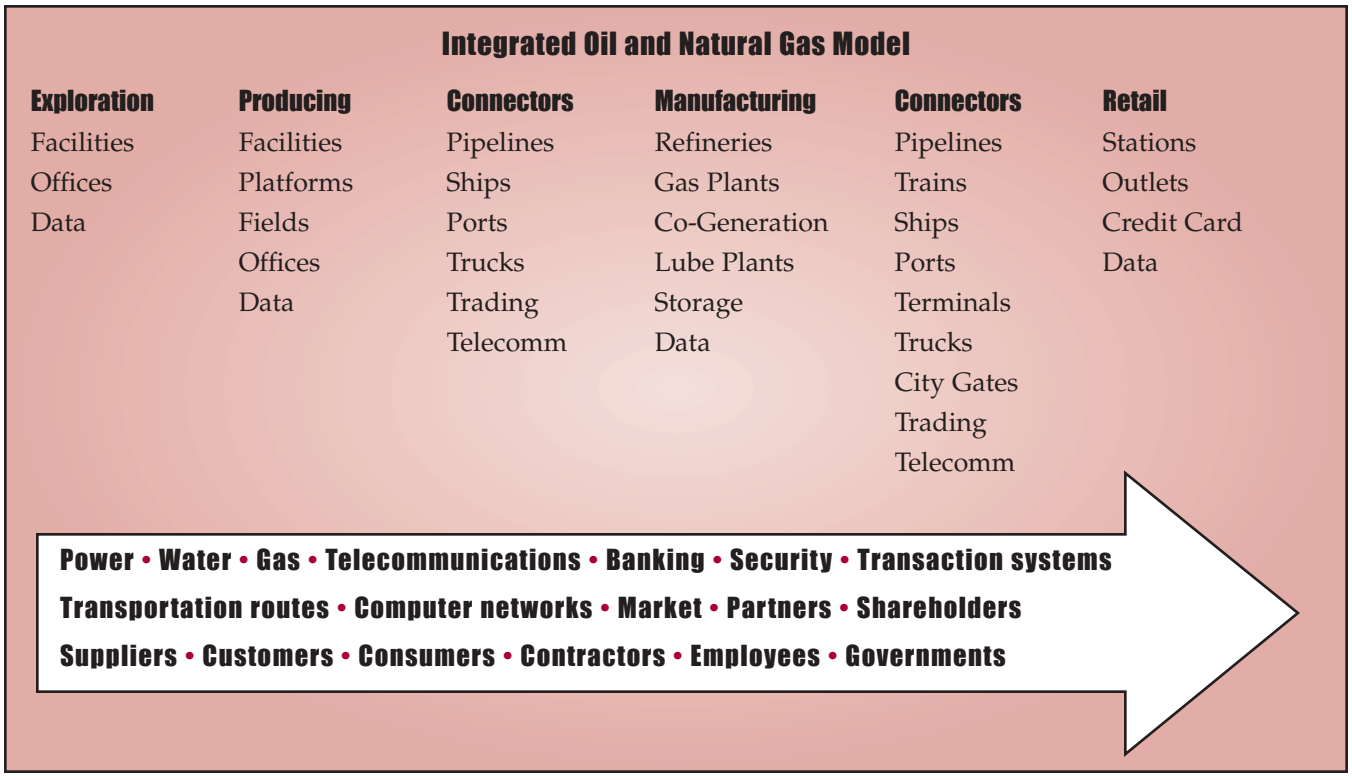

Figure 2-1. Flow of Raw Material into Commodities, and Then to Market

and telecommunications have rendered yesterday's systems obsolete and created bold new business models. Today's infrastructures are connected to one another, creating a complex network of interdependent systems. Coupled with advances in information technology and the transition to a new, cyber-based economic marketplace, these interconnected infrastructures now pose new security challenges for both the public and the private sectors that could threaten our national security.

Today's view of these infrastructures relies on the following:

- **Information Technology and Telecommunications.** The oil and natural gas infrastructures now rely on e-commerce, commodity trading, business-to-business systems, electronic bulletin boards, computer networks, and other critical business systems to operate and connect their infrastructures.

- **Globalization.** The oil infrastructure in particular cannot be examined from a domestic viewpoint alone. The oil industry has become multinational, evidenced by foreign supply dependence and ownership of former U.S. oil and natural gas companies by foreign companies.

- **Supervisory Control and Data Acquisition (SCADA) Systems.** The oil and natural gas infrastructures rely on and are increasing their use of automation technology to operate pipeline systems, refineries and other critical components.

- **Interdependencies.** The oil and natural gas infrastructures depend on other infrastructures such as electric power, information technology, telecommunications, banking and finance, transportation, and water to operate. Likewise, these other infrastructures depend on the oil and natural gas infrastructures.

Globalization—including foreign ownership of U.S. infrastructures, coupled with business dependence on information technology and telecommunications, and the dependence on foreign oil and natural gas supply—creates significant vulnerabilities to the U.S. oil and natural gas industries and the U.S. economy.

Figure 2-2 portrays the current model of the oil and natural gas industries' infrastructure. This infrastructure still contains its physical attributes, but oil, natural gas, and electric power are becoming more integrated as businesses. The oil and natural gas sector is more tightly coupled with other infrastructures, resulting in interdependencies, is heavily impacted by globalization, and relies on information technology and SCADA systems.

VULNERABILITIES, CONSEQUENCES, AND THREATS

The oil and natural gas industries have a successful record of physical security. In the past, even when faced with extreme events such as natural disasters, these industries have been able to minimize outages. Due to downsizing, increased asset utilization, and globalization of markets, a whole new set of vulnerabilities, consequences, and threats have been introduced through information technology and telecommunications dependencies.

In the past, most oil and natural gas vulnerabilities and threats could be negated by physical means. We used gates, guns, and guards (the fortress mentality) to protect our "critical assets"—and for the most part it worked. However, today the physical fortress can be rapidly by-passed by the "electronic key." It's a significant shift, analogous to the change between the old versus new way of business. For example, yesterday you had a paper check register and you balanced your account against the bank statement mailed to you each month. Today you can keep your entire account electronically: no paper register, no mailed statement. Many potential threats could corrupt or even delete your account information. These "cyber threats"

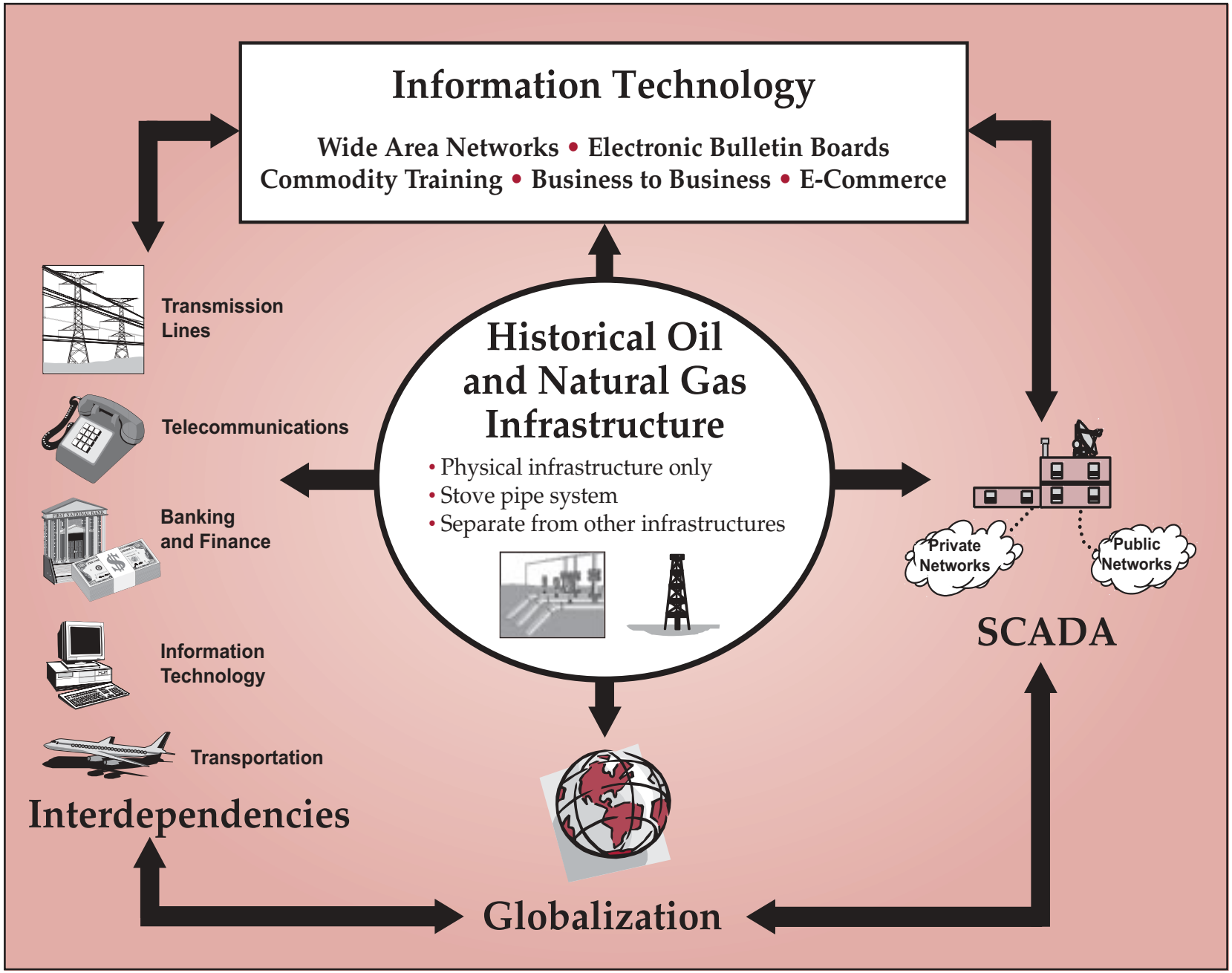

Figure 2-2. Profile of Current Oil and Natural Gas Industry

include hardware and software failures, human error, acts of disgruntled employees, outside hackers, and even something such as a merger with another bank and the struggle to consolidate systems. The consequence of these new threats is the problem of recovering the electronic register and supporting data. The best of class physical security cannot protect against these new cyber threats.

Cyber vulnerabilities have been around for several years. However, what has changed is significant business dependence on information technology and telecommunications as well as the increased awareness and ease of exploitation of these vulnerabilities. These vulnerabilities are widely known. Software vendors take products to market that can be flawed and often do not contain well-designed security interfaces. Detailed information on vulnerabilities and how to exploit them are distributed via hacker websites and chat rooms. The increases in denial of service attacks and computer viruses are examples of the consequences resulting from exploitation of these vulnerabilities. On the threat side, the advent of the Internet has provided a global platform for hackers, disgruntled workers, cyber terrorists, cyber activists, cyber militia, rogue nation states, and others to exploit cyber vulnerabilities.

For purposes of this study, vulnerabilities and consequences and their respective threats have been grouped into seven categories. They provide a framework to address the range of challenges that the sector faces today. The categories are as follows:

1. **Information Technology and Telecommunications.** Computers, the Internet, and high-speed telecommunications are critical ingredients in today's business place.

2. **Globalization.** The rise of the Internet and recent advances in telecommunications has boosted the surging train of a developing worldwide economy.

3. **Business Restructuring.** Changes brought on by globalization, competition, and technology advancements are reshaping the business environment.

4. **Interdependencies.** The oil and natural gas industries depend on one another and on other critical infrastructures such as electric power, information technology and telecommunications, and transportation.

5. **Political and Regulatory Issues.** The political and regulatory environment has tremendous impact on the oil and natural gas infrastructures.

6. **Physical and Human Factors.** The oil and natural gas infrastructures are composed of extensive physical networks to properly operate, as illustrated in Figures 2-1 and 2-2. Daily activities, including human error, have the potential to cause loss. Some examples of physical and human factors are oil, chemical, or biohazard spills; contamination; transportation (plane, train, truck, and ship) crashes; labor unrest; and political, social, international and domestic terrorism; organized crime; and hostile governments.

7. **Natural Disasters.** Occurrences in nature also have the potential to cause loss. Examples include storms (ice, rain), hurricanes, tornadoes, blizzards, floods, earthquakes, volcanic eruptions, and meteors.

These seven categories were rank-ordered and are presented in order of concern to the oil and natural gas sector. Information technology and telecommunications was identified as the highest overall concern to the sector while natural disasters were ranked as the lowest. These rankings were based on the perception of how well the industry is currently set up to deal with the vulnerabilities, consequences, and threats of each category. While natural disasters are a major concern to the industry, the industry has well-

established practices to handle these events, thus it was given a lower ranking.

Although each category has its own unique vulnerabilities and threats, some common themes regarding consequences exist. These themes portray the severity that these categories may have on the oil and natural gas infrastructure if not properly addressed. Each category, has the ability in some form to:

- Reduce the robustness of the oil and natural gas infrastructures
- Disrupt oil or natural gas service at a local, regional, or national level
- Disrupt national security and the U.S. economy.

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

If there is one vulnerability where a catastrophic event or failure can occur that could cripple any of the critical infrastructures, information technology and telecommunications is that area. In less than one generation, the information revolution and the introduction of the computer has changed how business and economies operate. Like other infrastructures, the oil and natural gas industries are becoming totally dependent on the availability of advanced telecommunication and information systems to connect customers, suppliers, and vendors with goods and services, including Internet-based links and transactions. Today's new business environment is shaped by the increasing role of technology and the resultant speed it generates in society as a whole. We are rapidly changing from an asset-based to a knowledge-based economy. It is an economy empowered by electronic technology, where anyone is only seconds away. The new business environment differs greatly from that of a few years ago and promises to be very different in the future, driven by continuous and rapid advances in information technology and telecommunications. The electronic revolution is providing the technologies and tools to complete the reshaping of the new global economy. E-commerce is a vast economic revolution that helps maintain market efficiency. In 1999, 2% of natural gas and 0.2% of electricity trades were conducted online. The use of this method of trading is conservatively projected to increase to 25% and 11%, respectively, in the next 2 to 3 years (*Natural Gas Intelligence,* April 17, 2000). For example, EnronOnline performed transactions valued at $336 billion of gross value in 2000, its first full year of operation.

While the new business environment offers new opportunities to the oil and natural gas infrastructures, it also presents serious challenges with regard to critical infrastructure protection. Increased adoption of cyber systems, SCADA, enterprise resource process systems, Automated Meter Reading, Internet-based transactions, just-in-time logistics, and e-commerce assist these infrastructures in operating more efficiently. However, oil and natural gas infrastructures have become dependent on these technologies before adequate processes have been developed to protect these systems, and thus, the infrastructures.

Vulnerabilities/Consequences

Information technology systems, while increasing efficiency and safety, also present new challenges. Keeping these systems running continuously despite potential outages due to hardware failures or software difficulties is, by itself, a significant challenge; however, new challenges are arising from internal, external, and system induced threats—making IT systems vulnerable to attacks.

The vulnerabilities are increasing in information technology. The following are examples:

- **We Can't Go Back.** The ability to go back to old manual methods is lost as we become reliant on these new systems. The new systems are automating work, and the current workforce

has no realistic manual backup process. As workers skilled in manual methods exit the workforce due to downsizing, retirement, and frequent job-hopping, etc., their knowledge is permanently lost.

- **Leap to New Technologies.** Due to competitive pressures, companies increase exposure by leaping into new technologies such as e-commerce and other electronic business tools without having appropriate security mechanisms designed and in place.

- **Shared or Joint Use Systems.** Many companies are creating shared or joint use systems for e-commerce. Failure of one of these systems not only has a negative impact on a member of the shared service, but also can cascade throughout the infrastructure, creating a significant vulnerability.

- **Foreign Access.** Mergers are creating ownership by non-U.S. companies. These actions are providing opportunities for foreign or nationally owned companies to access and adversely impact our infrastructures, creating additional electronic vulnerabilities.

- **Detachment from Consequences.** Systems are vulnerable because it is no longer necessary to be on the premises to attempt an attack. With today's advanced IT systems, people have the ability to attack from home, a business that sells computer equipment at the mall, or anywhere. Sometimes it is difficult if not impossible to determine where the attack originated. Rogue nations, terrorists, or other enemies are developing cyber warfare capabilities to attack infrastructures.

- **Security Features and Interfaces.** Because of the competitive pressures to bring products to market, vendors are rushing products to market quickly without effective security features and interfaces. The incomplete security features and interfaces create easily exploited vulnerabilities. Small, intermediate, or third-world companies who cannot afford information technologies security staff are extremely vulnerable. This vulnerability can be transferred between companies when they become contractors of, or venture partners with, a more mature company through interconnected systems.

- **Defective Software Security Features.** Existing products continue to be sold and installed while containing defects. Thus, new security patches arrive on a frequent basis, placing a burden on companies to keep IT systems and software up-to-date. Systems are vulnerable to attack until these known exploits are patched.

- **Computer Virus Attack.** The competitive nature of business requires involvement in electronic commerce. Consequently, exposure to computer viruses is an inherent risk. Computer virus prevention programs are reactive. New prevention programs only come after the viruses have infected IT environments.

- **Electronic Eavesdropping.** With today's widespread use of electronic devices, such as cell phones, Personal Digital Assistants (PDAs), and other wireless devices, communications can be easily intercepted and possibly altered.

- **Telecommunications Dependence.** Global telecommunications networks interconnect new economy systems. Failure in the telecommunications infrastructure will create significant impact on the oil and natural gas industries electronic infrastructure.

- **Potential Vulnerability.** Systems are primarily designed to rapidly manage and transmit, not protect, data. Consequently, they are inherently vulnerable to manipulation by inside and outside actors.

- **Activism.** There are interest groups with differing agendas that can negatively impact

business systems. The Internet provides them with a mechanism to bind together.

The price volatility and narrow profit margins that result from increased global competition have reduced the industry's time horizons for reacting to business and operation decisions from months to hours or even minutes. For example, a company decides to transfer fuel from storage to meet an unexpected demand from electric power generators. This action must be balanced with the overall system pressure, which requires many physical operating control changes throughout a system. Companies with remotely operated systems can adjust the necessary controls and rebalance the system in seconds, whereas companies that rely on manually operated controls cannot react to the changing supply needs of electric generators or major end-users. Today a typical refinery is almost fully automated; traders and automated controls run the refinery. Additionally, many facilities have installed "dual-use" power plants to take advantage of the price difference between oil and natural gas. Originally this was a manual switching process that took hours. Now it is an electronic process that takes minutes.

Today's global communications networks, which are crucial to operating businesses, rely on the Internet, Intranets, and Extranets tied to laptops, desktops, servers, firewalls, and routers. They depend on an open telecommunications architecture of satellites, fiber cables, microwave, phones, pagers, and cellular equipment. Consequently, a disruption to any of this equipment can threaten the reliability of the infrastructures.

Threats

Threats are real and growing and can cause system failures and system degradation. Threats can significantly affect the business or infrastructure, causing business failure, or failure to deliver services. Further inappropriate business decisions can occur if data have been changed or are not available:

- The FBI reports that cyber criminals allegedly penetrated almost all of the Fortune 500 corporations, costing the American economy approximately $10 billion a year.
- eBay lost $4 million in revenue during a 22-hour period when its systems crashed due to a software problem. The lost revenue cascaded into a loss of investor confidence of approximately $5 billion in eBay market capitalization.[1]
- The global use of malicious code, such as computer viruses, to disrupt business operations is increasing. The code is introduced into company computer networks by inside and outside actors.
- The level of hacker sophistication has evolved from the technically curious to malicious intent. Examples include identity theft, altering electronic fund transfers, modifying data used for investment/pricing decisions, and altering company web sites.
- Advances in information technology have permitted hacker tools to become easily available. The new tools are more sophisticated and easier to use, making them exploitable by a growing number of less computer literate individuals. For example, in 1999, a hacker took over control of a Russian gas system by penetrating the company SCADA system.
- Attacks from cyber systems can emanate from anywhere. Government sources report the increasing number of these groups developing cyber attack capability.
- A computer system failure can be closely linked with a business failure with potential cascading downstream effects.

[1] www.forbes.com/forbes/99/1213/6414322a.htm.

One of the most common forms and avenues of attack are social engineering techniques to get vital system access information that enables a malicious computer code to be placed in a company's computing environment or to exploit a misconfigured system. Further attacks are committed by exploiting remote access features and software bugs that have not been patched, and by using sophisticated programming tools to analyze the system for vulnerabilities. These attacks are delivered by exploiting system back doors, trusted links, Internet frontal attacks, and trusted insiders. These threats are further heightened by outsourcing and other "work displacement" arrangements that cause internal capabilities to atrophy. All of these threats circumvent the "physical fortress" a company has built.

GLOBALIZATION

The increasing use of the Internet and recent advances in telecommunications has led to new knowledge-based global economies, resulting in a fundamental shift in the business model. No single economy, including the United States, can be viewed in isolation. The global economy is rapidly bringing economic opportunity throughout the world.

The oil and natural gas industries along with their suppliers, customers, vendors, and related financial communities are all moving at an accelerated pace towards globalization. This is occurring through foreign ownership, consolidations of multinational corporations, joint ventures, strategic alliances, and partnerships with foreign governments. Even small natural gas distribution companies that previously operated in only one state in the United States a few years ago are undertaking business ventures across the globe. This has resulted in almost all U.S. energy companies, common suppliers, and contractors operating internationally. Conversely, foreign energy companies are also reaching beyond their borders to make financial investments in other countries, including the United States.

Globalization impacts the mix of owners, operators, suppliers, vendors, and customers of the oil and natural gas industries. It blurs the lines of demarcation making it difficult for companies to understand the changing market mix. The oil and natural gas industries used to understand their competitors, their customers, their suppliers, and their markets, and had some influence over each. Globalization changed all of that. Competitors exit and enter markets much quicker with no concern as to the impact on infrastructures.

Vulnerabilities/Consequences

Globalization is now an important factor in the growth of national economies. This newly formed model brings challenges that impact the oil and natural gas industries along with the infrastructures they support. Consequently, globalization adds complexity to companies dealing with differences in culture, work ethic, business protection, legal and regulatory issues, and political systems. Some examples are as follows:

- **Global Business Dependencies and Consolidations.** The oil and natural gas industries cannot be examined from a domestic viewpoint alone. The industry has become multinational, evidenced by foreign supply dependence and ownership of U.S. industries by foreign companies. For example, the financial crisis in Asia impacted U.S. oil prices and supply, OPEC decisions affect supply and commodity prices worldwide, and joint ventures and strategic alliances open the way for foreign interests to gain access to domestic information systems. These dependencies make the U.S. economy vulnerable to global influences that individual companies and governments cannot control.

  The U.S. economic vulnerabilities are impacted by industry consolidations involving foreign ownership of former U.S. companies. In some instances, foreign government-owned oil companies have acquired all or part of U.S. companies. This creates the possibility that

political considerations can affect domestic production and supply. Even an independent foreign-owned oil company can be influenced by a change in its government's relationship with the United States.

- **Business Inconsistencies.** Lack of consistent business and financial rules, legal frameworks, and international recourse create significant vulnerabilities in doing business globally. Thus, a company's limited control and legal recourse affect its ability to protect investments and manage risk, threatening supply and business continuity.

  Businesses are heavily dependent on information technology and telecommunications. However, many countries do not have sufficiently robust infrastructures to support efficient use of these technologies. This leads to inconsistencies in how technology is implemented, and can lead to loss of proprietary information and intellectual property resulting in the loss of U.S. business competitive advantage, and negatively impacting the U.S. economy.

  The current lack of international standards makes it difficult to implement critical infrastructure protection worldwide. The ability and willingness of governments to protect and enforce physical and cyber security also varies greatly.

- **Infrastructure Interdependencies.** Interdependencies are increasing in part from globalization. For example, a barrel of oil may be traded electronically hundreds of times before a U.S. company takes physical possession of it. For this to occur, information technology, telecommunications, energy services, banking and finance, and transportation infrastructures must operate effectively. All are much more critical because of increased business dependency on them to support globalization.

- **Emerging Privacy Concerns.** In order to do business in the global marketplace, it is essential that oil and natural gas companies have policies, procedures, and processes in place that demonstrate compliance with existing and evolving privacy legislation such as the European Commission Directive on Data Privacy.

- **Cultural Differences.** Many governments and economies are in varying stages of transition, which can cause instability. Different work ethics can affect productivity. It is difficult to vet workers, partners, and contractors in other countries. Not understanding and mishandling these cultural considerations can have devastating effects on a company's bottom line. Examples include the lost foreign investment in Venezuela when the country nationalized the oil and natural gas industry, and gross inefficiencies in company operations in Nigeria as a result of social unrest caused by government change and instability.

Threats

The following are examples of threats that could exploit the vulnerabilities enumerated above.

- Loss of foreign supply of oil and natural gas caused by:
  - Political or military actions of other countries
  - Terrorists/insurgents use of oil properties to promote their view, disrupt operations and supplies
  - Civil strife
  - Embargoes
  - Transportation problems.
- Foreign nationalization of a company's assets.
- Disruption or corruption of business information technology and telecommunications systems.
- Organized crime with undue influence or control over contractors, venture partners, or infrastructure components.

- Joint venture or strategic alliance partners whose companies were unable to be vetted can use the business relationship for undue financial advantage.

- In countries where there is a lack of legal structure, businesses are more at risk.

BUSINESS RESTRUCTURING

Today markets are global in nature as countries are forced by pressure from worldwide competition and access to cheap labor, to open their markets. With almost instantaneous access to information, markets are global, transparent, and, therefore, highly competitive. As a consequence, continuous cost reduction pressure is one of the new "antes" companies must make to play in the new business environment.

Prior to the last couple of decades, the oil and natural gas sector was relatively stable, composed of large integrated multi-national, and independent companies. The workforce was long-serving, loyal, highly experienced "old hands" who perceived that they had a "social" contract for employment resulting in a family model. Today mega-mergers, alliances, and joint ventures have resulted in organizations that no longer resemble those of the past. This restructuring has been facilitated by electronic information technology and the increased speed of transactions. This has given rise to the virtual organization, resulted in significant manpower downsizing, proliferated the number of global organizations, resulted in the transformation of service companies, and blurred the lines between traditional oil, gas, and power companies. Therefore the work environment has become less stable, pressures have built to do more with less, knowledge and experience have been "outsourced," and the "social" employment contract has been broken.

Companies are continually focused on cost reduction. This has led to business re-engineering, outsourcing, and downsizing, and an increasingly diverse, multi-national workforce consisting of employees, contractors, consultants, vendors, and suppliers. This results in reliance on contract and service level agreements to have work performed.

Vulnerabilities/Consequences

Restructuring has produced new business models for the oil and natural gas industries that have created significant vulnerabilities.

Changing Employee Social Contract

One of the major ways that companies reduce cost is by reducing the number of employees. Thus, reducing the number of employees through layoffs, early retirements, and outsourcing of functions have reduced these labor costs. This has resulted in a break in the "social" contract, which has reduced employee corporate commitment and increased the possibility of exploitation of vulnerabilities for their own gain. Consequently, numerous companies have suffered attacks and/or have lost intellectual property due to former employees angered at the company. The workload on remaining employees has increased, leading to further employee dissatisfaction ("do more with less").

This same action has caused employees to not expect to spend a career with one company. For the same reason, newer employees do not expect to stay with one company but to move within the industry or within other industries.

These corporate actions have caused employees to focus more on their own welfare rather than on the welfare of the corporation, creating real vulnerabilities. Numerous instances have surfaced where employees have taken intellectual property with them as they migrated to other companies. Additionally, disgruntled employees have sabotaged company operations. The trend of continued cost cutting and outsourcing will continue to drive employees to think of their welfare before the welfare of the company.

Outsourcing

Cost reduction and a focus on core competencies has driven corporations to outsource many functions, some of which are critical to the operation of the company. There are many vulnerabilities due to outsourcing of these critical functions which include:

- Employees separated due to outsourcing are often hired by contractor companies to do the same job for the same company, resulting in conflicting loyalties. Employees of outsourced functions do not have the same level of corporate commitment, as a full-time employee would possess.

- Outsourcing companies may have less secure procedures and policies. This exposes the client to additional vulnerabilities. They may not vet employees to the same standard that a company does, or on a recurring basis.

- Outsourced employees are rotated between different companies served by the contractor firm. It is difficult to stay current with background checks, photo IDs, keycards, passwords, and other security procedures. It is also difficult to keep training current. By the time a contractor learns a role, that contract employee is rotated to a new assignment. This can also lead to proprietary information being taken by a contract employee to a competitor.

- Critical functions, including information technology and telecommunications, have been outsourced, which potentially creates major vulnerabilities. Contract employees of outsourcing companies have inside knowledge of system architecture, security features of networks, systems, and desktops, and their vulnerabilities. This sensitive information can be used against a company whether the contractor employee is employed by the contractor or a subcontractor. With all company operations supported by an outsourced information technology vendor, the failure of that vendor could result in catastrophic consequences with limited means for restitution.

Joint Ventures and Strategic Alliances

Joint ventures and strategic alliances bring with them significant potential vulnerabilities:

- Intellectual property that is not part of the venture or alliance is difficult to protect as companies share information through shared systems.

- Individuals of different companies participating in a venture or alliance form close relationships. These do not always end when the venture or alliance ends, placing intellectual property at risk through personal contact.

Just-In-Time Logistics

Technology changes have allowed near-real-time information transfer and transactions, permitting companies to significantly reduce their bench stock. This concept has promoted alliances with vendors to furnish stock as required on a near-real-time basis. The lack of ability to perform in a timely manner to meet a company's needs can have severe consequences. Companies rely on both their vendors and their supporting transportation infrastructure to provide timely equipment and services. By providing vendor access to their information systems, companies become dependent on this vendor for efficient business operations.

Changing Business Model

Historically, the oil and natural gas industries have had clearly delineated boundaries, but rapid shifts have made it difficult to categorize these industries. Oil and natural gas companies are merging with other oil and natural gas companies, with electric power companies, and with other industries (e.g., telecommunications). Some companies are even selling energy assets and getting out of the energy business altogether. Today's oil and natural gas companies may own assets in electric power, water, information

technology, telecommunications, and banking and finance. The integration of all energy infrastructure components is making it more difficult to address critical infrastructure protection on an industry-by-industry basis. Some recent events illustrate these points:

- A major energy provider is selling off its energy assets to obtain higher profits in the telecommunications industry.
- Oil and natural gas companies are investing millions in e-commerce activities, which compete with physical capital investments.
- It is easier to enter the energy market. Companies that once were not involved in the industry now eagerly enter into the business. Even Amway—a marketing company—sells energy services.
- Foreign ownership of U.S. energy systems is increasing.

Threats

The primary threat from business restructuring is the workforce, whether employee, contractor, consultant, vendor, or supplier. Their potential lack of loyalty to a company along with their inside knowledge gives them the capability and opportunity to exploit the vulnerabilities described above.

INTERDEPENDENCIES

The global Y2K threat pointed out how interdependent companies have become. Interdependencies are dependencies on other infrastructures. Figures 2-3 and 2-4 illustrate some of these dependencies. For example, both infrastructures require information technology and SCADA systems to automate operations. The integration of information technology and telecommunications into business is creating a critical interdependence between infrastructures, i.e., banking

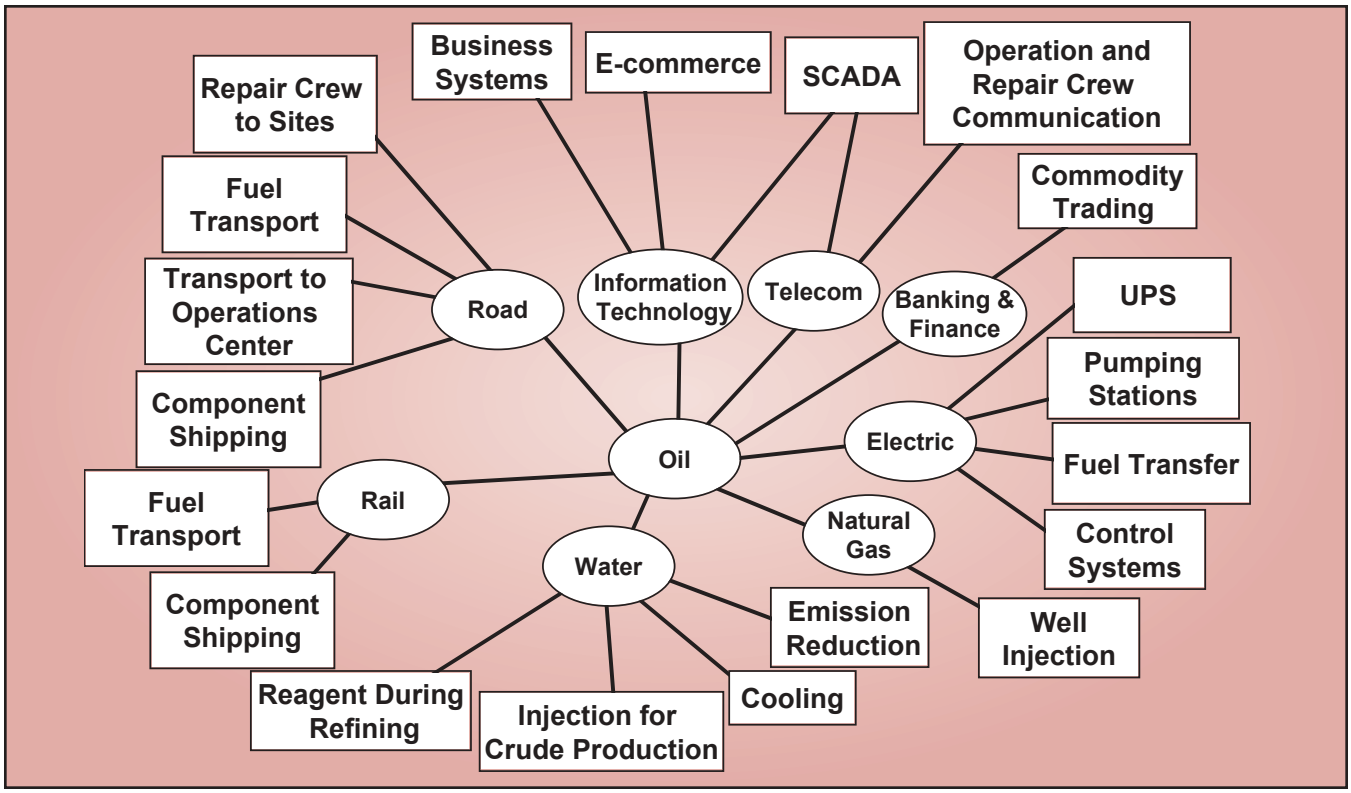

Figure 2-3. Examples of Oil Interdependencies

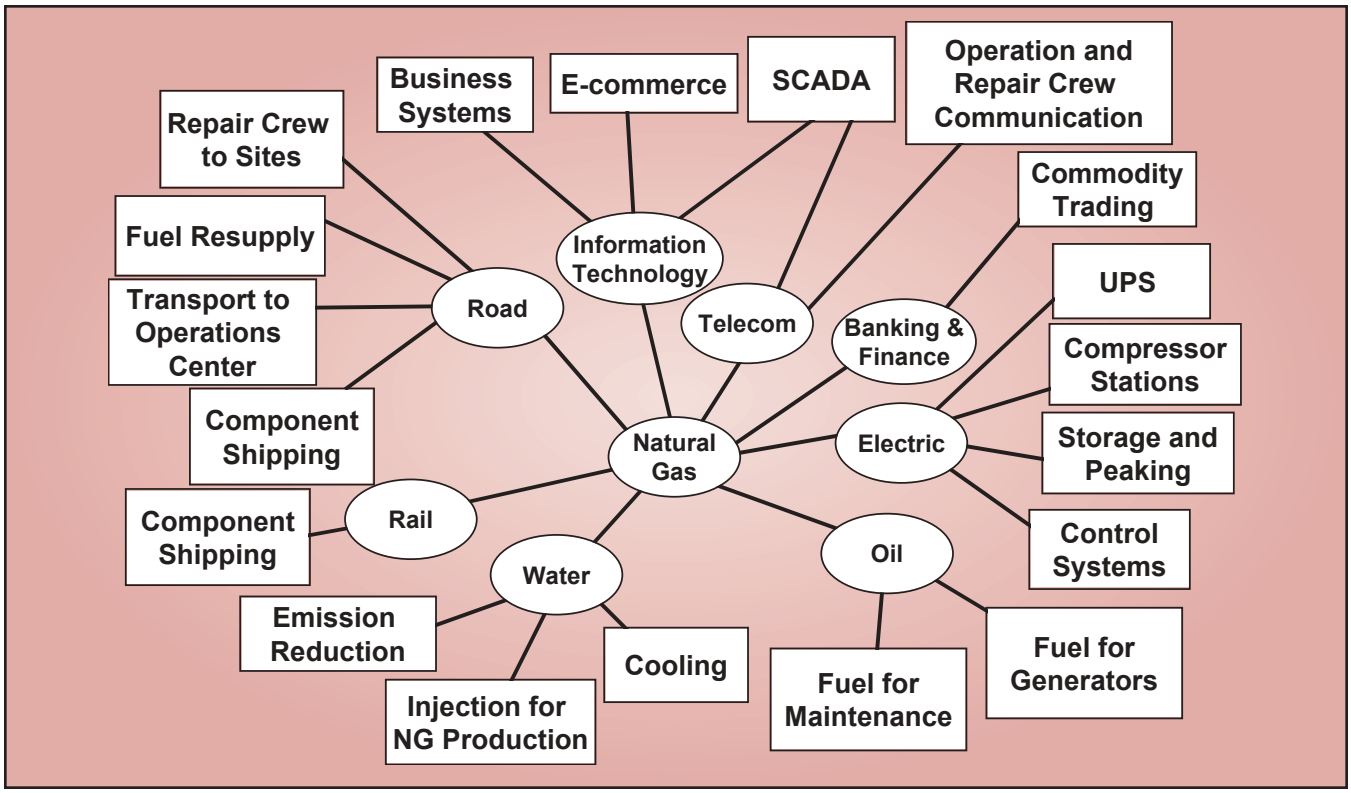

Figure 2-4. Examples of Natural Gas Interdependencies

and finance, power, water, oil and natural gas, transportation, information technology, and telecommunications. Over time, these infrastructures have become critically interlinked. This reliance will continue to grow because of globalization and business restructuring.

Vulnerabilities/Consequences

As indicated above, the interdependence of all infrastructures in today's new business environment creates critical vulnerabilities. For example, most new natural gas appliances use electronic ignition and will not operate without electricity.

Electric Power

Today, the majority of businesses are dependent on information technology and telecommunications infrastructures. Therefore, if the power infrastructure is unable to deliver, these critical infrastructures fail and global business falters. The electric power infrastructure increasingly relies on natural gas for electric power generation. New generation capacity from natural gas is projected to be over 90% (EIA).

Transportation

Given business dependence on just-in-time logistics, a failure in the transportation infrastructure can significantly disrupt business.

- Pipelines move large quantities of raw feedstock and finished products throughout the oil and natural gas infrastructure. It can take days to move petroleum and natural gas from production/processing locations to end-use markets. Delays or problems in pipeline operations can lead to shortages and price spikes.

- Besides pipelines, petroleum products rely on barges, rail and trucks to move products to end-use markets. Delays or problems can have similar impacts as pipeline disruptions.

- Transportation is needed to dispatch repair crews.

- Because of dependence on foreign oil and product supply, a breakdown in the transportation infrastructure negatively affects the U.S. economy and infrastructures.

Common Utility Corridor

A common utility corridor that contains overhead electric power transmission lines, buried gas pipelines, and telecommunications cables, dramatizes interdependencies. Co-locating infrastructures makes them more susceptible to a single incident such as explosion, fire, flood, and seismic events, as well as sabotage.

National Defense

The Department of Defense, other executive agencies, and defense contractors are dependent on the oil and natural gas sector providing appropriate products to meet national defense requirements.

Threats

Interdependency threats are a new and evolving component of critical infrastructure protection and one of the most difficult to understand. These interdependencies in the new business environment can be described as follows:

- **Cascading.** A failure in one infrastructure leads to a failure in another infrastructure. (For example, an electric power failure can shut down an oil pumping station.)

- **Escalating.** The outage duration time from an infrastructure outage is increased from an outage in another infrastructure. (For example, a problem in the transportation infrastructure could increase the time of an oil or natural gas crew to respond to an outage, increasing the restoration time.)

- **Common Mode.** An incident has the potential to impact multiple infrastructures. (For example, natural gas, electric, oil, and telecommunications components all may exist in a shared right-of-way.)

- **Marketplace.** E-commerce links multiple infrastructures through the dynamic marketplace it creates. (For example, denial of service attacks can impact multiple infrastructures.)

- **Compounding.** The compounding of infrastructure failures by unforeseen events like natural disasters. (For example, a critical pipeline rupture coupled with a seismic event and unseasonably warm weather leads to failure of the electric generation system.)

POLITICAL AND REGULATORY ISSUES

Political and regulatory uncertainty makes it difficult for U.S. oil and natural gas industries to make long-term strategic decisions. Investments in infrastructure, i.e., pipelines, refineries, and wells, are all based on an individual company investment strategy. Regulatory changes can make it difficult to fully estimate the return on these investments and assess potential liabilities causing some companies not to make critical investments to improve their infrastructures. Thus there is a conflict between the national desire to have a robust, resilient infrastructure, that can withstand attack or be rapidly reconstituted, and individual company's investment strategies. This significantly impacts critical infrastructure protection.

Often the government reacts to social and political pressure based on single incidents, which can lead to legislative and regulatory changes that have a significant impact on the oil and natural gas industries. To facilitate critical infrastructure protection at the national level, industry and government must find solutions that are acceptable to all stakeholders.

Vulnerabilities/Consequences

Implementation of regulations and policies can have unintended negative consequences on infrastructure protection.

The following are examples of regulatory and political issues that have hindered the oil and natural gas infrastructures:

- The Olympic Pipeline is an example of the impact of regulatory and political forces. Olympic Pipeline Company operates a 400-mile pipeline system in the states of Washington and Oregon and delivers approximately 300,000 barrels per day of refined petroleum products from four refineries.

  On June 10, 1999, a segment of 16" pipeline in the city of Bellingham, Washington ruptured, spilling an estimated 3,600 to 6,600 barrels of gasoline and resulting in 3 deaths. It took 18 months before the Department of Transportation allowed operations to continue. This tragedy has led to an outcry in the state of Washington and in Washington, DC for stricter federal pipeline regulations. In 2000, several pipeline safety bills were introduced in the U.S. Senate and House of Representatives. The bills called for periodic integrity testing of pipelines, higher penalties for safety violations, increased training for pipeline operators, and greater participation by states and communities in pipeline oversight. The Senate Bill, with minor amendments, was passed in February 2001 (the Pipeline Safety Improvement Act of 2001).

- The creation of the northeast heating oil reserve was a reaction by government to the higher prices of heating oil supplies in the northeast that occurred during the winter of 1999-2000. The reserve was created during the later part of 2000 when heating oil prices were high because of low commercial inventories and cold weather. The filling of the reserve during this period further contributed to the tight heating oil situation.

- Transmission pipeline companies in the oil and natural gas sector face considerable opposition to new pipeline construction. The expressed concerns relate to safety, environmental, congestion, land use, and loss of property value. Critics point to the relatively few pipeline accidents that have occurred as reason enough to not allow or severely restrict new pipelines.

  – Many strong "not in my backyard" groups have been formed to fight new pipelines. The National Pipeline Reform coalition formed in 1998 has supported several of these opposition groups.

  – The difficulties encountered in building new pipelines limit competition and result in many existing pipelines operating at or near capacity. Any disruption in operations can affect regional supplies and result in price spikes.

- The Clean Air Act Amendments of 1990 mandated that risk management plans (RMP) be written for various industrial facilities, including oil refineries and natural gas processing facilities. These plans require certain facilities to prepare "worst case scenarios" that included very sensitive offsite consequence analysis (OCA) information. Because Congress failed to provide any specific mandate on the dissemination of RMP information in the Clean Air Act, and because there was no generally applicable law that would prevent the Environmental Protection Agency (EPA) from doing so, the EPA was considering posting the RMP information on the Internet, making it publicly available. Widespread opposition to the EPA's plan was raised by law enforcement and intelligence agencies concerned that making such information so widely available raised the dual threat of the information being used for terrorist acts and economic espionage. In the face of this opposition, the EPA reconsidered and decided not to place the most sensitive portions (the OCA information) on the Internet.

Threat

The past has shown that legislative and regulatory solutions have had unintended negative consequences. Because information technology is a new and major part of oil and natural gas industry operations, new laws, regulations, and policies could have greater unintended negative consequences than in the traditional settings. Government and industry must work together to understand the effects of such legislation and regulation to prevent similar negative effects.

PHYSICAL AND HUMAN FACTORS

The oil and natural gas infrastructures are very capital intensive with significant physical assets. For example, a single drilling platform may cost $50 million or more, whereas deep-water platforms cost 10 times that amount. Tankers can cost millions of dollars, with LNG tankers being the most expensive vessels outside of military vessels. Transmission pipelines can cost up to $1 million per mile to construct and that does not include the compressor or pumping stations, which can exceed $40 million and are required at approximately 50-mile intervals. Petroleum refineries, gas processing centers, tank farms, gas storage fields, odorant facilities, and distribution systems are also costly investments. Some of these facilities, such as petroleum refineries, are not even being built anymore because of environmental constraints, capital requirements, and poor economic returns.

The U.S. oil and natural gas infrastructures are vast and numerous. Table 2-1 identifies some of the major U.S. infrastructure components. They are comprised of extensive and sophisticated equipment that in turn comprises the backbone of these infrastructures. Thousands of independent operators are the driving force that connects these infrastructures together.

Vulnerabilities/Consequences

The physical vulnerabilities of these infrastructures vary between components. For

Table 2-1
Physical U.S. Oil and Natural Gas Infrastructure Components

Fuel Cycle	Oil Infrastructure Components	Natural Gas Infrastructure Components
Production	602,200 wells	276,200 wells
Gathering	74,000 miles of crude pipeline 30,000 miles of gathering pipeline 74,000 miles of product pipeline	45,000 miles of gathering pipeline
Processing	161 petroleum refineries	726 gas processing plants
Transmission	74,000 miles of crude pipelines 74,000 miles of product pipelines	254,000 miles of transmission pipeline
Storage	2,000 petroleum terminals	410 underground storage fields 54 complete LNG facilities
Distribution	616.5 billion ton miles of pipelines 295.6 billion ton miles water carriers 27.7 billion ton miles motor carriers 16.7 billion ton miles railroads	981,000 miles of pipeline

example, the production side is more diverse with hundreds of thousands of wells that produce oil and natural gas. As a result, the loss of a specific well would be considered a low vulnerability. Table 2-2 defines low, medium, and high vulnerability rankings adapted from the Critical Infrastructure Assurance Office definitions.

Figures 2-5 and 2-6 are vulnerability rankings for the oil and natural gas infrastructures. There are several components that are ranked high. This means that a potential component loss could cause a major disruption of service.

These high-ranking components include oil and natural gas transmission pipelines, oil pumping stations and natural gas compressor

Table 2-2
Vulnerability Rankings

Low – Key assets that if damaged could cause disruptions with local impacts of short duration.

Medium – Key assets that if damaged could cause disruptions that would have regional impacts. These disruptions would last long enough to cause end users hardship, economic loss, and possible loss of human life.

High – Key assets that if damaged could cause major disruptions that would have regional and possibly national or international impacts, and of sufficient duration to cause death and end users major hardship and economic loss.

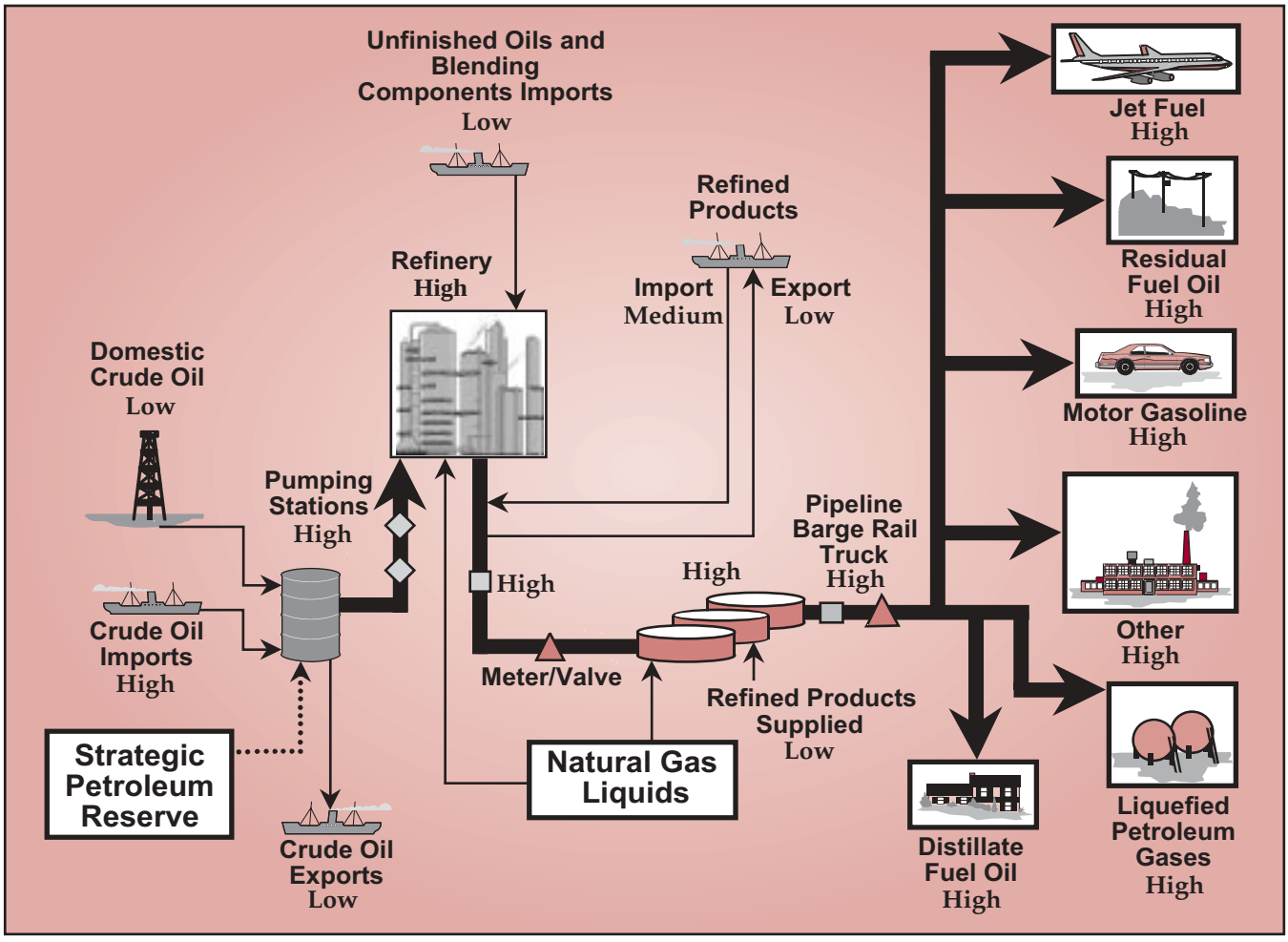

Figure 2-5. Physical Vulnerabilities of the Oil Infrastructure

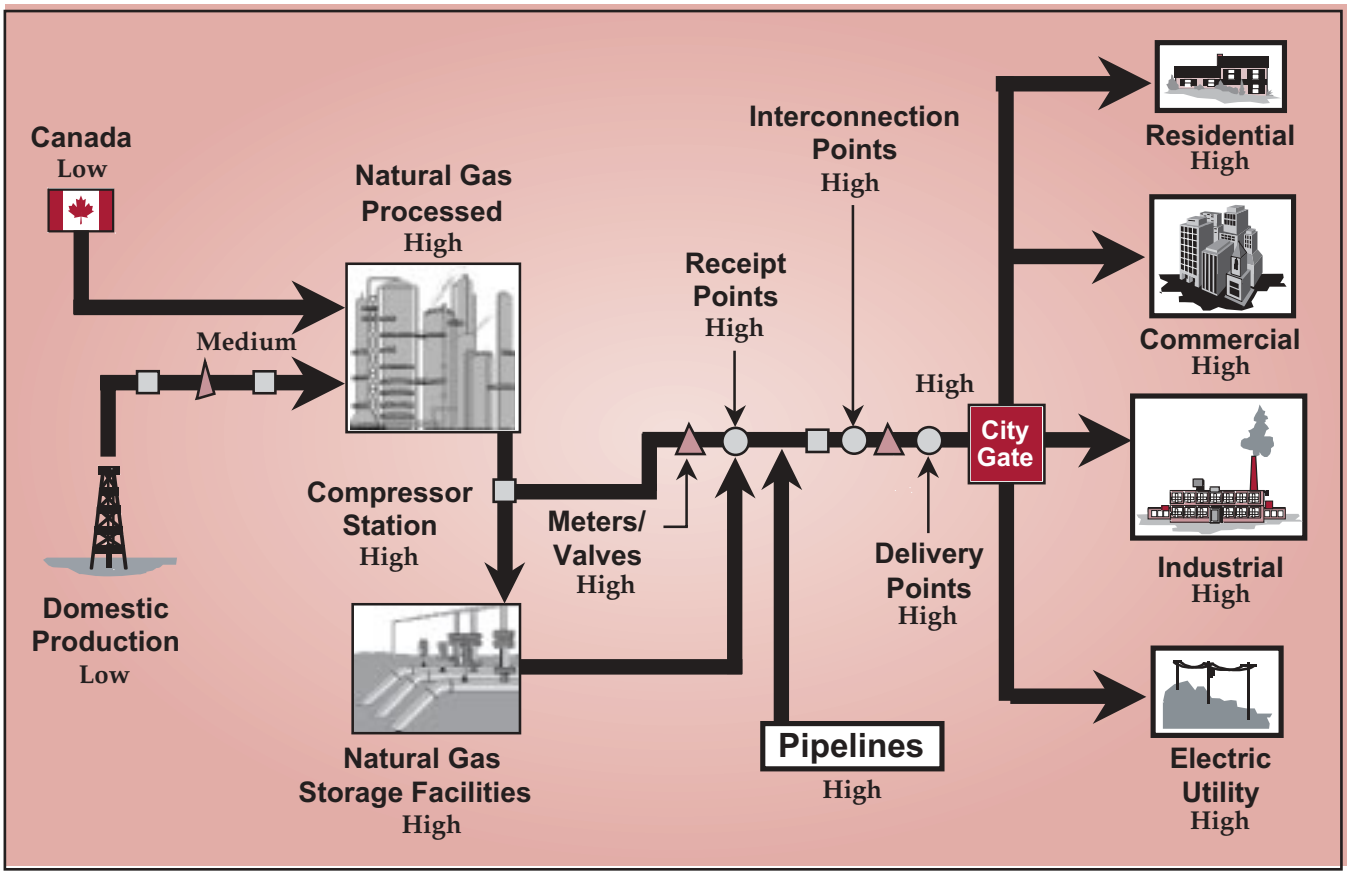

Figure 2-6. Physical Vulnerabilities of the Natural Gas Infrastructure

stations (used to flow commodity through pipelines), storage, and distribution. Disruptions of these components could result in infrastructure outages.

- **Damage to Underground Pipelines.** Underground pipelines are vulnerable to accidental damage. Construction equipment is the most common cause even though pipelines are easy to identify from their open right-of-ways and pipeline markers. Additionally, these open right-of-ways and pipeline markers make targeting these critical assets relatively easy to entities with hostile intentions.

- **Increased Utilization.** Information technology has allowed physical assets to be utilized at significantly higher levels. As physical asset utilization increases, the consequences of the loss of a single asset increases the impact of an outage. The stress of higher utilization can lead to infrastructure failure.

- **Transportation Failure.** The blockage of a shipping channel in 2000 led to a withdrawal of oil from the Strategic Petroleum Reserve because two major refineries were going to use up their on-site inventories before the shipping channel was back in service.

- **Delayed Restoration.** Due to just-in-time logistics, some companies are reducing their inventory of spare parts, which could increase outage duration times.

- **Automated Remote Facilities.** The industry has become dependent on remote automated production or transportation facilities. Reaction time to reach and repair these remote facilities could be extensive.

Threats

The range of threats covers a wide spectrum, from an outage at an infrastructure component, caused by inadvertent human error that causes minimal infrastructure disruption, to an event or societal change that threatens an entire infrastructure. The oil and natural gas infrastructures are comprised of an extensive range of physical assets, many which span thousands of miles, and may be difficult to protect.

Some examples of threats are oil, chemical, or biohazard spills; pipeline breaks; accidental third-party damage; natural disasters; contamination; transportation (plane, train, truck, and ship) crashes; labor unrest; disgruntled workers; violent political activists; international and domestic terrorism; organized crime; and hostile military action.

NATURAL DISASTERS

The oil and natural gas industries respond quickly and well to natural disaster threats. Their response to natural disasters such as the Loma Prieta and Northridge earthquakes, Midwest floods, and hurricanes such as Hurricane Andrew is outstanding. The industry, often supported by government, quickly rallies together by providing emergency equipment and personnel on an informal basis.

Vulnerabilities/Consequences

Occurrences in nature have the potential to cause substantial loss. Storms (ice, rain), hurricanes, tornadoes, blizzards, floods, earthquakes, volcanic eruptions, and meteors are occurrences that can exploit vulnerabilities of physical systems. These actions can have major consequences with destruction of physical facilities, failure of systems, and loss of life. Within the United States, industry and government are well prepared to deal promptly and effectively with these vulnerabilities.

However, as the U.S. oil and natural gas industries have more and more critical assets abroad, the vulnerability may increase due to immature infrastructures in other countries where those assets are located. Therefore, the ability to respond quickly and thoroughly to such natural disasters can be impaired.

Additionally, industry downsizing, increased interdependencies on other infrastructures, high asset utilization, industry restructuring, and inconsistent business continuity planning make it more difficult in the future to maintain this excellent track record. The network of people who had the relationships that enabled the industries to support each other is rapidly diminishing, as are the working relationships between companies to permit such actions. Even internally, company downsizing and dependence on information technology is causing a reduction of skilled labor increasing the difficulty to mitigate impacts from natural disasters.

Threats

Threatening acts of nature include hurricanes, cyclones, typhoons, earthquakes, volcanic eruptions, floods, tornadoes, and meteor impacts.

FINDINGS AND CONCLUSIONS

- Information technology and telecommunications are the areas where a catastrophic event or failure could cripple any or all of the critical infrastructures.

- A failure in the telecommunications infrastructure will create significant impacts to the oil and natural gas industries because of local and wide-area networks interconnecting new economy systems.

- The ability to go back to old methods can be lost, as oil and natural gas companies become reliant on these information technology and telecommunication systems. Because of the

change in organization, the workforce is no longer as experienced or as skilled as before, and it often lacks the ability to operate systems without cyber tools, thereby limiting the capability to return to older manual methods.

- Failure of joint or shared use systems for e-commerce not only has a negative impact on a member of the shared service, but also can cascade throughout the infrastructure creating a significant vulnerability.

- Information technology and telecommunications systems are vulnerable to externally initiated events because it is no longer necessary to be on the premises to launch an attack, or to create an interruption.

- Rogue nations, terrorists, or other enemies are developing capabilities to attack cyber infrastructures.

- Competitive pressures can often lead to the use of immature technologies and can introduce significant vulnerabilities to enterprises and the infrastructure.

- The oil and natural gas industries are faced with a continuous stream of patches and fixes to correct product security defects of information technology and telecommunications systems that businesses are highly dependent upon.

- U.S. energy components (i.e., oil, natural gas, electric power, other energy sources, and their transportation modes) are converging with each other in the marketplace. The National Petroleum Council recommends that in the implementation of Presidential Decision Directive 63, all components of U.S. energy sectors be recognized as a single energy infrastructure.

- Globalization is a key to the growth of national economies, but adds complexity to companies dealing with differences in culture, work ethics, business protection, legal and regulatory issues, and political systems.

- U.S. economic vulnerabilities are impacted by industry consolidations involving foreign ownership of former U.S. companies.

- Companies are continually focused on increased efficiencies and cost reductions. This leads to business re-engineering, outsourcing, and downsizing. The result is a blend of employees, contractors, consultants, vendors, and suppliers, some of which are located in foreign countries, with less corporate commitment.

- The integration of information technology and telecommunications into business is creating a critical interdependence between infrastructures, i.e., banking and finance, power, water, oil and natural gas, transportation, information technology, and telecommunications.

- Interdependency of infrastructures is a new and evolving component of critical infrastructure protection and one of the most difficult to understand creating threats to businesses.

- The lack of consistent business and financial rules, legal frameworks, and international recourse, create significant vulnerabilities in doing business globally.

- To facilitate critical infrastructure protection industry and government must work together to find solutions.

- The oil and natural gas industries respond quickly and well to threats created by natural disasters and other physical events. Historically, although individual companies have not experienced widespread emergencies they have done a good job in responding to problems, and in restoring service to customers.

- The oil and natural gas infrastructures are comprised of an extensive range of physical assets,

many which span thousands of miles, and may be difficult to protect.

- The converging of energy infrastructure components is making it more difficult to address critical infrastructure protection on an industry-by-industry basis.
- The oil and natural gas industries are statutorily required to disclose potentially sensitive information to government. Congress and the government agencies must ensure that appropriate mechanisms are in place to prevent such information from being released to unauthorized entities.

CHAPTER 3

Risk Management

Risk is a component in all human endeavors and is a word that means different things to different people. For most people, risk is the "possibility of suffering harm or loss."[1] In risk management, risk is defined as "a combination of the probability of an adverse event and the nature and severity of the event."[2] Therefore, to measure risk it is necessary to consider both the probability that an adverse event will occur and the consequences of that event.

Important components of risk management include asset valuation, vulnerability and threat characterization, risk assessment, and the evaluation of risk abatement options. Risk management uses all these components to evaluate risk and combine them with other relevant factors (e.g., costs, legal mandates, etc.) to select an appropriate risk abatement[3] strategy.

The vulnerabilities and threats that the oil and natural gas industries face are increasing and more complex. Outsourcing, e-business, anonymous transaction-based operations, and adoption of non-traditional business relationships further complicate risk management, placing businesses at more risk.

Many companies in the oil and natural gas industries use aspects of risk management today in addressing risks of capital investment, interest rates, new ventures, and price volatility. The types of vulnerabilities and threats, and the nature of risks faced in this information age, which is the driver for the new global economy, are accelerating rapidly. Therefore, the key to managing risk is to develop new prevention strategies and establish processes to manage negative consequences.

RISK MANAGEMENT AS A TOOL TO ENHANCE CRITICAL INFRASTRUCTURE PROTECTION

A factor impacting risk abatement for critical infrastructure systems is the traditional tendency of many industries to manage physical security and safety risks in a focused and serious manner when the risk is recognized in advance or following a significant event. The recent trend in the energy sector is to address security issues in a more proactive manner. Security takes on increasing importance as the cost of cyber events increase. A study of risk management activities in private-sector companies indicates that the intensity of security risk management varies.[4] A cost-effective strategy is a sustained level of security that is adequate to recover from past security breaches and establish measures to prevent future adverse events.

The oil and natural gas industries have done a positive job in addressing traditional operational risks. Today the introduction of information

[1] American Heritage® Dictionary of the English Language: Fourth Edition, 2000.

[2] Presidential/Congressional Commission on Risk Assessment and Risk Management, 1997.

[3] Abatement is all activity or techniques that are deployed to eliminate, reduce, or transfer the consequences of financial loss, damage, or destruction of assets (a program of activities).

[4] Science Applications International Corporation. Organizations and Business Case Model for Information Security. Prepared for the Office of the Manager, National Communications System (OMNCS) Customer Service and Information Assurance Division, Information Assurance Branch (N53). August 26, 1997.

technologies has increased risks. For instance, the cost to recover from the "ILoveYou" virus is estimated to exceed $1 billion. Respondents to a Computer Security Institute survey reported a combined loss in excess of $377 million during 2000, an increase of $112 million over 1999.[5]

It is apparent that electronic infrastructure losses such as these are escalating with time. The benefits of a preventive strategy include fewer incidents and reduced costs per incident. Such a strategy can more than offset increased sustained costs of security programs. When added to the increased value associated with a culture of disciplined secure operations, such a strategy is a major contributor to a sound risk management program.

Many industries already have formalized programs to assist in mitigating risks. Understanding key components of risk management strategies and programs of other industries provides insight and a starting point for developing strategies to assess and reduce risks in the new economy. The chemical process industry, the commercial nuclear power industry, and the National Aeronautics and Space Administration (NASA) have always had risk assessment programs. Each industry, due to critical events, has reevaluated their risk management programs. The oil and natural gas industries have risk management processes in place for traditional operations and the introduction of and reliance on electronic infrastructure suggests that risk management processes need to be reevaluated and extended.

THE OIL AND NATURAL GAS INDUSTRIES' PERSPECTIVE

Historically, oil and natural gas industry managers have dealt with a wide range of physical risks, currency risks, interest rate risks, product liabilities, increased competition, loss of public confidence, and loss of investor confidence. In the new economy, cyber risks add to the complexity of risk management. The complexity for a company to understand their risks arise in part from the increasing dependencies and the interconnectedness congruent to the new business environment. Companies inherit vulnerabilities and threats of their partners and suppliers, resulting in a blurring of risk boundaries. Wall Street analysts and bond raters are including information systems valuation in corporate ratings.

Most industry managers view risk largely in terms of the likelihood and/or the extent of financial loss. Although industry managers cannot reduce all financial risks to zero, they strive to reduce risks to an acceptable level.

Industry managers generally focus on and have more experience dealing with legal, financial, and technical/operational risks, than with risks involving the accidental loss or sabotage of the interconnected electronic networks on which they, their customers, and their suppliers depend. This is the case primarily because operational losses, as well as the cost of their abatement, can be measured in dollar values. Cyber risks to corporate infrastructures are much harder to estimate because they involve intangible, highly uncertain potential losses. Despite this difficulty, processes similar to those used to manage operational risks can be used to manage cyber and other critical infrastructure risks.

A basic risk management process that could be used by the oil and natural gas industry involves six steps (see Figure 3-1). These steps involve characterizing assets, describing vulnerabilities and threats, performing risk assessments, developing risk abatement options, selecting risk abatement activities, and implementing these activities. The six steps are then repeated after an appropriate period of time (e.g., yearly, every other year) or as warranted by changes in the risk environment (e.g., development of new technologies, emergence of new threats).

[5] Computer Security Institute, March 2001 Computer Crime and Security Survey. For a free copy of this report, go to http//www.gocsi.com/fbi_survey.htm.

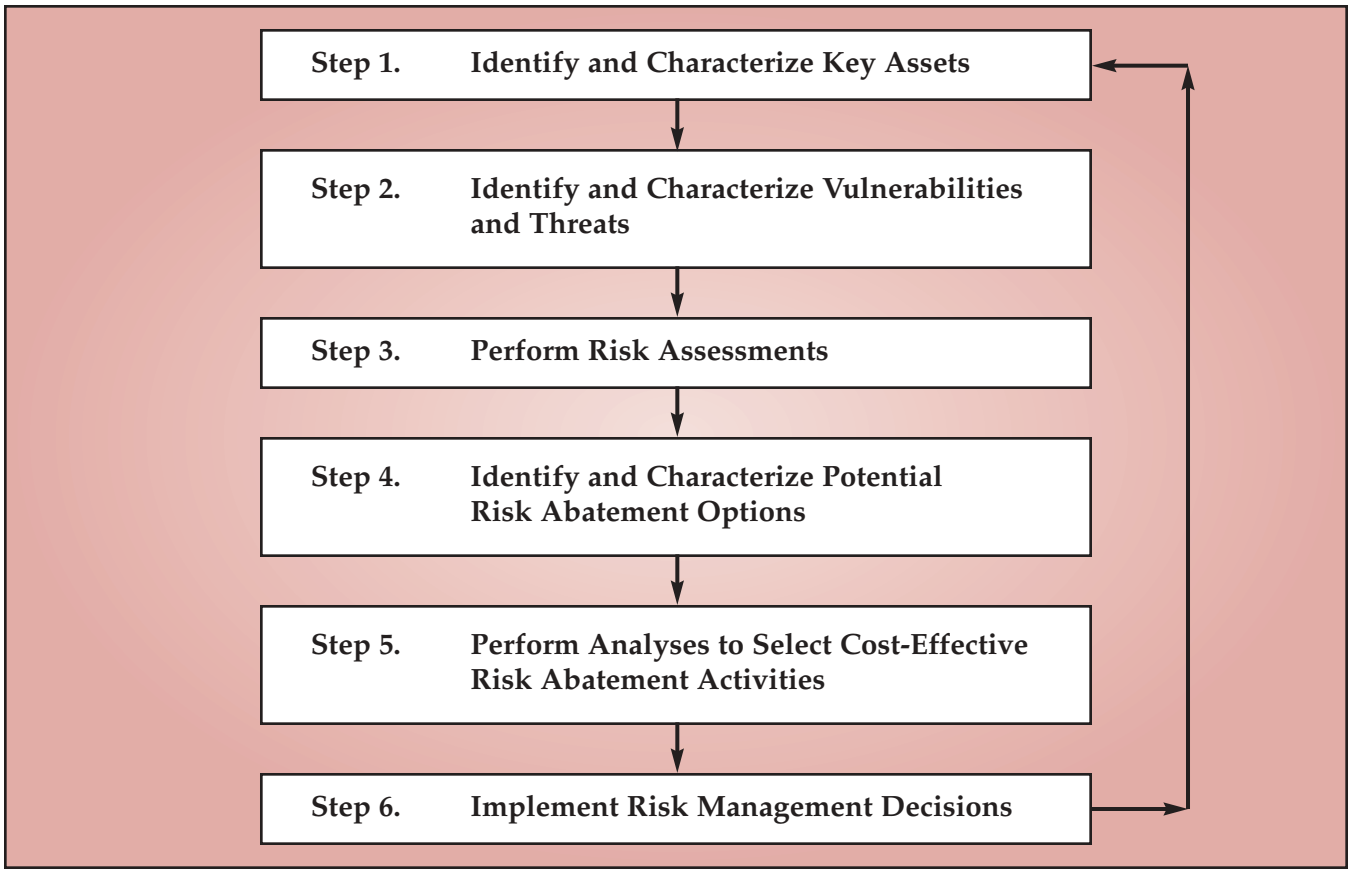

Figure 3-1. Example of Risk Management Process

Although most risk management programs follow the same basic steps, the level of effort and the complexity of different programs can vary from industry to industry. In simple programs, one or two key people might complete most steps in the process in a few days. In programs that call for in-depth analyses, a team of analysts might work for months to complete the same steps. For most uses, cost and schedule constraints are a major factor in determining the level of effort and sophistication of a risk management program. Often, a simple program is sufficient for providing meaningful risk management guidance to decision makers.

Identifying and Characterizing Key Assets (Valuing Assets and Estimating Losses)

The first step in the risk management process is to identify and put a value on each of the key assets of the organization. These key assets can be people, facilities, services, processes, programs, etc. Next, the "impact of loss" for each of these assets is estimated. This is a measure of the loss to the company if the asset is damaged or destroyed. A simple rating system based on user-defined criteria can be used to measure the value of the asset (e.g., very low, low, moderate, high, extremely high) and the impact of its loss. In a more complex risk management system, the value of an asset and impact of loss can be calculated in monetary units. These values may be based on such parameters as the original cost to create the asset, the cost to obtain a temporary replacement for the asset, the permanent replacement cost for the asset, costs associated with the loss of revenue, an assigned cost for the loss of human life or degradation of environmental resources, costs to public/stakeholder relations, legal and liability costs, and the costs of increased regulatory oversight.

Losses due to cyber viruses and computer hacking are especially difficult to estimate. The International Computer Security Association estimated North American losses from the "ILoveYou" virus at about $1 billion (June 2000). The results of the annual Global Information Security Survey (July 2000), conducted by Information Week Research and PricewaterhouseCoopers assisted by Reality Research & Consulting, indicated that in the prior year U.S. companies had losses of $266 billion, 2.7% of U.S. GDP, from computer viruses and hacking. This same study indicated worldwide business losses of $1.6 trillion, including lost productivity and sales opportunities.

The March 2001 report of the Computer Security Institute on their year 2000 Computer Crime and Security Survey confirms that the threat from computer crime and other information security breaches continue unabated and that the financial toll is mounting. According to their report, the average financial loss for the three years 1996–1998 was $120 million. In contrast, the loss in fiscal year 1999 was $265 million and in 2000 the loss escalated to $375 million.

The risks associated with the new cyber business environment are difficult to define or postulate. Subsequently, resultant corporate losses are challenging to estimate. That is, an event can now have unanticipated consequences outside of the business sector in which it occurs. For example, the "ILoveYou" virus impacted oil and natural gas cyber and physical systems. In addition to cyber systems being slowed down from the e-mail bombardment, a petroleum refinery was completely shut down from the virus. Cascading failures due to interdependencies are currently beyond the control of single corporations or even a single economic business sector. Thus, collaboration among industry sectors is essential if risks are to be managed at acceptable cost.

The importance of an asset determines the level at which it should be protected from cyber or other security threats. Some assets, such as trade secrets or control systems (SCADA), may be so important to a company that their loss cannot be financially mitigated, for example, by insurance. These assets must be protected from exposure to cyber loss. Traditionally, preventive security measures have been accomplished through isolation. For example, many corporate information and technology centers maintain proprietary and time-sensitive information. Such centers require two or more independent authentication security measures to achieve access. In the oil and natural gas industries, many companies use similar protection strategies for assets considered critical to operations.

Because some assets, such as administrative assets or word processing software, are easily obtained or replaced, the need for protection is limited. Thus, only minimal resources are needed to abate their loss, or the risk of their loss. Most corporate assets fall somewhere in between.

Identifying and Characterizing Vulnerabilities and Threats

The second step in the risk management process is to identify and characterize vulnerabilities and threats. This involves carefully considering a wide range of vulnerabilities and threats. Vulnerability assessments identify weaknesses, review the effectiveness of current security measures to protect assets, and suggest additional measures to reduce risk. Frequent vulnerability assessments are essential to ensure that new vulnerabilities, particularly those associated with cyber systems, are identified and addressed in a timely manner. Use of third parties to periodically assess vulnerabilities can augment and provide objectivity to in-house audits. To further identify vulnerabilities, some companies use "red teams" to proactively "assault" their company's principle physical assets, information systems, and networks.

Examples of factors commonly addressed in vulnerability assessments are shown below:

- Cyber
  - Network Security – Internal and External View
  - Data Security
  - Systems Administration – User or System, Desktops and Servers
  - Data Classification and Disposal
  - Detection and Response – Time to React
  - Policies and Procedures
  - User Awareness and Compliance
  - Information System Dependencies & Interdependencies
  - Vendor, Partner, Supply Chain
- SCADA
- Physical
  - Access Controls, Administration of Badges, Key Controls
  - Loading Dock/Deliveries
  - Mail Service
  - Barriers, Sensors, Closed Circuit TV
  - Guards
  - Social Engineering
  - Environmental and Safety
  - Incident Response Plans
  - Policies and Procedures
  - User Awareness and Compliance
- Security Awareness Program
- Internal and External Interdependencies.

To manage risk, it is important to understand the threat environment in which assets operate. Threat agents exploit vulnerabilities to cause loss. The changing nature of threats makes threat assessment a dynamic process. The timely collection and analysis of threat information is complicated by numerous information sources, lack of accessibility (for example, classified government intelligence), and the lack of an information-sharing mechanism. Frequent threat assessments and timely sharing of information enhances industry's ability to deal with the rapidly changing threats. A number of factors that should be considered in the evaluation of threats include:

- Existence of threat agents with capability to access the target
- Capability of the threat agent to cause harm (demonstrated or assessed)
- Intent to cause harm (demonstrated, stated, or assessed)
- History of activity by the threat agent has been observed
- Targeting of a facility in the past, or current credible information of activities by potential threat agents
- Existing security environment's impact on the capability of a threat agent to be successful in exploiting a vulnerability.

Threat levels are determined by the degree to which combinations of these factors are present. The more factors that are present, the higher the level of threat.

Typical threat agents include:

- Disgruntled employees and insiders
- Criminals
- Hackers
- Competitors

- Malicious software
- Natural disasters or human error
- Activists
- Terrorists.

Threat is determined by the presence, capability, and opportunity-to-act of threat agents.

Evaluations of threats and vulnerabilities are combined to estimate the probability of loss of an asset. Loss histories are also helpful in estimating probabilities, but addressing new threats and vulnerabilities, associated with cyber systems where no history exists, requires collective expert judgment. As a result, it is easier to estimate probabilities and consequences of loss for physical assets than for cyber assets. The rapid changes in cyber technology, evolving information systems, and the expanding application of both cyber technology and information systems increase vulnerabilities. Moreover, business processes increasingly depend on timely access to information. Increasing interdependencies and interconnectivity increase both the vulnerabilities and the consequences of potential corporate loss.

Performing Risk Assessments

The third step in the risk management process is to perform a risk assessment using the information collected on assets, vulnerabilities, and threats. The goal of this process is to be able to assess the risks associated with each key asset. This involves considering a wide range of identified vulnerabilities and integrating probability and impact information. For example, the probability component in a risk estimate must consider the:

- Probability that an attempt will be made to exploit a vulnerability. Just because vulnerability exists, does not mean that an attempt will be made to exploit that vulnerability.

- Probability that once made, an attempt to exploit vulnerability will be successful. Some attempts to exploit vulnerability fail because of the action of existing safeguards, serendipity, or ineptitude.

- Probability that a given level of impact will be experienced. If vulnerability is successfully exploited, there are ranges of negative outcomes that can occur. For example, the actions of a hacker who has penetrated a computer system can range from relatively benign to extremely destructive.

In some cases, a single vulnerability will drive the overall risk estimate. In other cases, a series of different vulnerabilities may contribute substantially to the overall risk level. Once a company has a clear picture of the risks to its assets, it can begin to identify problem areas and see where risk abatement measures may be most effective in reducing risks to acceptable levels.

A number of different risk assessment tools and techniques can be used to estimate risks. Again, the type of tools depends on the resources and time available to conduct the risk assessment. All approaches require a fair measure of documentation. The adequate documentation of input into risk assessments is required so that the work can be reviewed, conclusions assessed, and information stored for future reevaluations.

Identifying and Characterizing Potential Risk Abatement Options

The fourth step in the risk management process is to identify and characterize risk abatement options. Industry managers typically consider a number of abatement options for cost-effective risk reduction. Risk abatement activities generally focus on five different areas: the deterrence of threat agents, protection from threats by reducing or eliminating vulnerabilities, mitigation activities to reduce the consequences of a potential loss event, effective crisis management to reduce the severity of an event while it is going on, and restoration to rapidly recover from an event (see Figure 3-2).

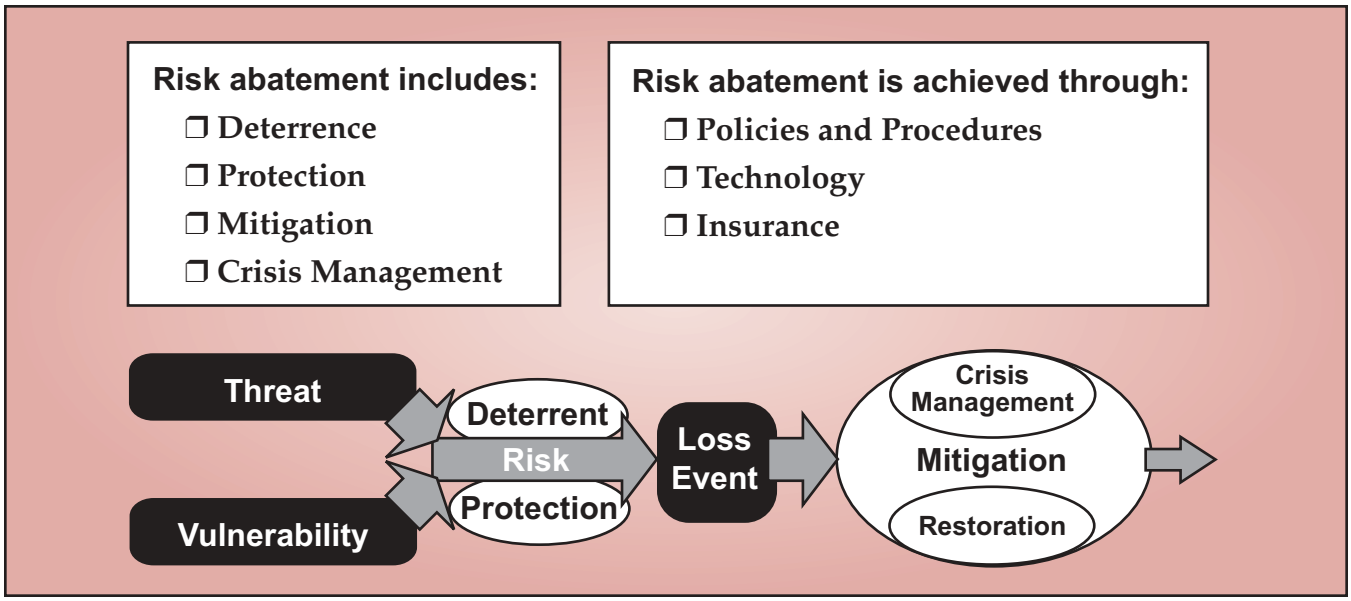

Figure 3-2. Risk Abatement Measures in the Loss Process

Risk abatement approaches include the following examples: Assets can be armored to protect against loss, or resilience can be built in. In the oil and natural gas industries, pipelines are not armored. Rather, pipeline control systems are designed for early detection of failure. Control centers, on the other hand, often have multiple layers of security protection, but limited backup should control systems be breached.

Some infrastructure threat agents are deterred by effective law enforcement or international legal actions. Protection of assets and crisis management is enhanced through adoption of policies and procedures, technologies, and institutional supports that reduce corporate and business sector vulnerabilities. Adoption of abatement technologies and institutional cooperation can facilitate rapid restoration of service. Insurance mitigates financial losses.

Protection measures, such as the isolation of assets reduce the likelihood of a loss event, but do not change the level of impact, should the asset be lost anyway. Some have both a protection and mitigation component. For example, anti-virus software reduces both the likelihood of loss as well as the impact. Mitigation measures, such as insurance, apply only after initiation of loss. Mitigation reduces the consequences of an event and/or provides financial compensation or other redress for the loss. Thus, the use of risk abatement measures to protect assets, or their financial value, is an effective management tool, before, during, and after a loss.

In identifying and characterizing risk abatement options, it is important to be thorough and identify options that have different levels of effectiveness and cost. While low cost options are desirable, risk abatement options come with a range of initial and annual operational costs. Effectiveness also varies, so that while some options might almost totally eliminate a vulnerability, others may only reduce risk by lowering the probability that a vulnerability can be exploited (e.g., by requiring a more sophisticated attack to breach a vulnerability) or by reducing potential damages. By providing a range of risk abatement options, decision makers can choose the one that has an appropriate impact and an acceptable cost-to-benefit ratio.

In evaluating risk abatement options, it is important to assess not only new approaches, but to also evaluate existing risk abatement activities.

In some cases, there may be cost-effective alternatives to existing risk abatement strategies. In other cases, existing risk abatement activities may not be needed if the vulnerabilities they address no longer present the same degree risk that they did in the past.

The cost of various risk abatement measures can be reduced through cooperative industry efforts. Development of standards is one effective way of both reducing the cost of risk abatement as well as ensuring that business partners require comparable levels of risk management. Examples of standards that focus on information technology security are the current ISO/IEC 15408-1 standard (International Standards Organization/International Electrotechnical Commission) and ISO 17799 standard. Security topics are addressed by a number of existing industry standards, but not to the degree necessitated by the new economy. Considerable effort will be necessary to formulate a cohesive set of standards that appropriately augments corporate and industry practices to enhance infrastructure protection in the new economy.

Performing Analyses to Select Cost-Effective Risk Abatement Activities

The fifth step in the risk management process is to select risk abatement activities for implementation. In business, the resources that may be applied to risk abatement are limited. Other business needs compete for the same funding. After carefully reviewing the risk environment, decision makers must determine an acceptable level of risk for the company. Decision makers then need to review the available risk abatement options and determine which suite of options should be implemented.

In some cases, the appropriate risk management decision may be to continue existing risk abatement programs. In other cases, it may be necessary to modify existing risk abatement programs or implement new risk abatement options. The goal is to select the most cost-effective suite of risk abatement options that will reduce risk to an acceptable level. The more risk abatement options the decision makers have to choose from, the more flexibility they will have in putting together a successful risk management program.

Implementing the Risk Management Decisions

The sixth and final step in the risk management process is to implement risk management decisions. This is the essential step in the process. There is little benefit derived from a risk management program unless it is executed in an effective and efficient manner. This typically involves:

- Preparing plans and procedures for implementing risk abatement activities
- Assigning and training staff to perform risk abatement activities
- Monitoring risk abatement work to make sure the planned program is being carried out and risk reductions are actually occurring
- Maintaining an active surveillance of the threat, vulnerability, and risk abatement environment to identify changes that may be occurring that could warrant modification of risk management activities.

FINANCING LOSSES THROUGH INSURANCE

All oil and natural gas companies carry some form of property and liability insurance, whether self-insurance, mutual insurance, or insurance purchased from the various global insurance markets. Property insurance compensates a company financially for the loss of its own insured assets. Liability insurance compensates a company when it becomes legally obligated to pay for damages caused to the assets of others.

All insurance relies on the ability to establish a monetary value for the loss that places an insured in a position commensurate with that preceding the occurrence of the loss or insured event. For proprietary, confidential business information or intellectual property, monetary value is often established based on investment costs. For example, unless intellectual property is under license agreement or contract for sale at an established price, establishing a market value, the property is not insurable for what it might be worth in the future. That is, companies cannot insure against speculative lost opportunities. Thus, intellectual property or other business sensitive or proprietary information lost as a result of cyber incident may not be insurable under existing insurance industry principles.

Insurance against business-interruption may reimburse a company for damages resulting from a cyber incident if a monetary loss can be established. Because business opportunity costs are difficult to evaluate, however, loss of ability to do business, with no collateral property damage, is usually not insurable, although the value of lost work time may be.

Little case law currently exists that addresses civil wrongs (torts and breach of contract) resulting from a company's infrastructure collapse due to cyber events or other disruptions. However, as documented in this report, the fact that cyber incidents will occur is predictable. And, to a certain extent, they can be mitigated. Thus, in the future it is expected that companies which fail to exercise due diligence in protecting themselves and their cyber partners against attacks could be found legally negligent.

The impact of a corporate infrastructure failure due to a cyber event may also cause breach of contracts for oil and natural gas companies that promise delivery of specified quantities of products on specified schedules. Under these circumstances, liquidated damages or other compensations may be extraordinarily high, and may not be insurable.

Insurance companies are beginning to offer specialized policies applicable to cyber risks. Companies purchasing such insurance typically are subject to a risk assessment by the insurer and are required to implement specific network security measures. Because of limited legal case his-tory and inadequate loss experience, however, premiums for such policies are generally expensive and the available coverage is limited. Maturation of insurance offerings to "acceptable" levels requires completion of all the fundamental risk assessment elements discussed here. Furthermore, it requires that risks, including vulnerabilities, threats, and loss consequences, and abatement measures are well documented and understood.

Corporate insurance to protect against cyber losses may be valuable to corporate stockholders. But the transfer of risk that insurance provides does not help the global economy. The financial strength of certain major oil companies, on their own, may exceed the insurance capacities in the global insurance markets. As such, corporate insurance protection will have minimal impact to global consumers of the oil and natural gas industries.

Although consumers may have no legal recourse against the oil and natural gas industries if products and services are not available, the global economy can be brought quickly to a halt if the distribution infrastructure collapses.

THE Y2K EXPERIENCE

In a real sense, Y2K presaged future risks associated with the new economy, and Y2K preparations demonstrated the first major multi-industry, multi-national response to cyber-related risk. In effect, Y2K provided a worldwide cyber example, and a success story, of the value of a global community response to a common threat.

Companies associated with the oil and natural gas industries organized teams to address Y2K

risks. In addition, the federal government both challenged industry to validate that Y2K risks were low and monitored validation progress. Congress provided special assistance through the passage of the Year 2000 Information and Readiness Disclosure Act of 1998 and the Y2K Act. Specifically, these acts limited risk and authorized exemption from antitrust statutes to enable industries to share information and address common vulnerabilities. Recently, legislation has been introduced to provide some of the same protections to coordinated industry action intended to reduce risks associated with e-commerce.

The following Y2K lessons are applicable in the new economy:

- Federal legislation can facilitate industry-wide collaboration to address threats and vulnerabilities.
- Systemic cyber vulnerabilities can be shared without compromising business integrity or competition.
- Collaboration on infrastructure vulnerabilities, especially cyber vulnerabilities, can reduce both cost and risk.
- Interdependencies that require coordinated attention can be successfully addressed.

FINDINGS AND CONCLUSIONS

- The key to managing risk for the oil and natural gas industries is to develop prevention strategies and to manage consequences of incidents when they occur. However, new strategies and best practices are needed to protect against information loss or the breakdown of critical infrastructures in the new economy.
- Risk boundaries are being blurred by the expanded use of network-based communications and computing, and by adoption of business models that use information technology to streamline organizations and their operations.
- Costs of cyber risks to corporate infrastructures are difficult to estimate because they involve intangible, highly uncertain potential losses.
- Risk management will be enhanced by the adoption of consistent industry standards for cyber security management.
- Companies in the oil and natural gas industries benefit from conducting periodic vulnerability assessments of their own systems and operations, both physical and cyber.
- Companies need to perform assessments of, or be made aware of, their partners' vulnerabilities. Additionally, companies need to understand and assess the vulnerability to their systems from unknown third parties.
- In the highly interconnected business cyber world that exists today there are many risks that cannot be defined or postulated. Consequently, a risk management system needs to be developed to address these unknowns.
- Companies cannot insure against speculative lost opportunities. Thus intellectual property or other business-sensitive or proprietary information lost as a result of a cyber incident may not be insurable under existing insurance industry principles.
- As a tool for managing risk, information sharing is a vital element of enhanced prevention and control for the oil and natural gas industries.
- Collaboration, enabled through federal legislation for Y2K, allowed cost-effective reduction of risk through cooperative programs and information sharing across industry. Comparable federal legislation would enable similar cost-effective risk management programs addressing critical infrastructure protection.

CHAPTER 4

Response and Recovery

Response and recovery planning, in conjunction with timely information on threats and vulnerabilities, plays a major role in mitigating business risks.[1] Such contingency planning provides companies with the necessary review of potential unexpected business consequences, and the opportunity to preplan and test responses to them. Year 2000 preparations brought into sharp focus the need for contingency planning beyond the traditional scope of emergency response and recovery. In today's new business environment, response and recovery planning must address the following:

- Industry reliance on information technology and telecommunications
- Business restructuring
- Interdependencies
- Legislative and regulatory uncertainty
- Natural and man-made incidents.

The oil and natural gas industries have experienced many physical failures. Perhaps the worst was an explosion in Texas City, Texas, on April 16, 1947. A ship exploded at a dock, causing fires and detonations in the surrounding refineries and chemical plants. At least 581 persons were killed and approximately 3,500 were injured. As a result of such incidents and other process failures, businesses have developed contingency plans for responding to and recovering from these physical incidents and their causes.

[1] **Response** is the immediate emergency, law enforcement, defense, or other crisis management response to an incident to protect life, health, safety, and property. **Recovery** is the action taken after the initial response to rebuild homes, replace property, resume employment, restore businesses, and reconstitute life.

CURRENT STATE OF INDUSTRY RESPONSE AND RECOVERY PLANNING

Physical Infrastructure

Historically, most companies understand and are able to handle their own physical infrastructure problems. Prudent business practices require industry to quickly respond to physical incidents caused by natural events such as earthquakes and hurricanes, and man-made events such as vandalism, criminal activity, terrorism, accidents, etc. Typically these incidents result in local consequences. Today increased use of automation, increased interconnectedness, just-in-time business models, and interdependencies can potentially result in regional, national, or international incidents and impacts. These broader consequences pose additional challenges to effective response and recovery planning, incident response, and consequence management.

Government regulations in the area of safety often dictate how businesses prepare and execute their response and recovery plans. For example, the Department of Transportation Office of Pipeline Safety requires that pipeline companies have formal emergency response plans, and annual drills to test those plans. Another example is the National Response System, which provides a mechanism for emergency response to discharges of oil into navigable waters of the United States and releases of chemicals into the environment.[2]

[2] The National Response System is described in the National Oil and Hazardous Substances Pollution Contingency Plan (NCP), found in Title 40 of the Code of Federal Regulations, Part 300.

As part of that system a National Response Team was created. The National Response Team's membership consists of 16 federal agencies with responsibilities, interests, and expertise in various aspects of emergency response to pollution incidents. The Environmental Protection Agency (EPA) serves as chair and the Coast Guard serves as vice-chair of the National Response Team. Company contingency plans to deal with pollution incidents are required to include the involvement of either the Coast Guard or EPA.

For the traditional types of natural disasters, the Stafford Act dictates how the Federal Emergency Management Agency (FEMA) responds, and funds local recovery operations. The act also provides criteria through which states may request and acquire federal funding for their recovery operations.

At the international level, maritime law provides rules for insurance, shipping, and salvage of cargo on the high seas. Countries have also adopted oil spill response and chemical process safety regulations to protect their environments. Insurance is being used globally to mitigate consequences and fund response and recovery operations that might become necessary.

International agreements and national programs can serve to protect against serious supply interruptions. An example of an international agreement was the formation of the International Energy Agency in the wake of the 1973-74 oil crisis. The U.S. Strategic Petroleum Reserve was created to provide an inventory buffer against an interruption in petroleum supplies.

Mutual aid programs are methods that industry and local governments use in preparation for response and recovery to large incidents. These have been and will continue to be rather well established practices and networks for mutual benefit. For example, companies located along the Houston Ship Channel have mutual aid agreements for fire fighting equipment and personnel. Most terminal and refining companies enter into similar types of agreements. In addition, most communities surrounding large airports or other large public facilities have mutual aid pacts with the owner/operator to facilitate response to large-scale fires, medical emergencies, or crashes.

Other examples are Intermat, Inc, and the Edison Electric Institute (EEI), which provide their members with a mechanism to obtain skilled workers and materials to augment their own capabilities during an emergency. Intermat provides a Mutual Emergency Materials Support (MEMS) system. EEI's process provides a framework for requesting assistance, governing principles and insurance aspects, as well as forms (checklists, letters, contracts, invoices, definitions, etc.) to facilitate the communications between the requestor and the company providing the mutual support.

There are less formal agreements between oil and natural gas companies for "borrowing" supplies when an emergency arises. These agreements are generally verbal and based on a "hand shake" in field environments. The types of supplies involved cover anything from pipe to compressor parts. These informal agreements are generally based on personal contacts in field offices. As people leave the workforce and new personnel or automated systems take over, these informal agreements are less likely to occur. Pre-planned mutual aid agreements are more efficient and dependable.

Gaps in Physical Infrastructure Response and Recovery

From the perspective of the oil and natural gas industries, individual companies have not experienced widespread emergencies such as the outages historically experienced by electric utilities. Individual companies have done a good job in responding to problems, and in restoring service to customers.

The concerns of public and environmental groups as they relate to an incident, create public

relations issues and often cause the government to react in unanticipated ways. The number of local, state, and federal government agencies that respond to incidents can create confusion for the owner/operator in providing an incident command and control process as part of their response and recovery plan. This confusion may delay the restoration of service. Government response to public reaction to incidents can result in unfavorable outcomes for industry and other stakeholders. An example is the incident experienced on the Olympic Pipeline, described in Chapter 2, where government oversight resulted in it taking 20 months from the time of the incident to re-establishment of partial service.

While some companies have long experience in dealing with regional, national, and international physical infrastructure incidents, the globalization of entire industries has resulted in new players who may not be as well prepared. There is a strong incentive for these new participants to develop or enhance response and recovery plans suitable for dealing with widespread incidents. Cooperation between industry and government can expedite the response and recovery from incidents impacting physical infrastructure disruptions.

Cyber Infrastructure

Wide uses of information and communications technology are generating new challenges for response and recovery planning. Contingency plans need to include the cyber dimension that is pervasive in the new business environment. The complexity and scope of response and recovery operations can easily exceed the capabilities that any one company has for dealing with a crisis (scope of consequences, interdependencies, cascading effects, rapid spread, regional, national, and international impacts) in this area.

Companies have become reliant on cyber systems to operate physical infrastructures, provide e-commerce, and perform general business transactions. Thus, cyber incidents can affect automated computer controls of physical infrastructures, integrated telecommunications, and interdependent distribution systems, which may result in physical damage. Moreover, failures of general business, trading, and other e-business systems can lead to significant losses. Based on experiences from the 1989 San Francisco earthquake, if a company experiences a major incident and does not recover its critical business processes within five to seven days, or the consequences overwhelm its ability to respond, the company could be forced out of business. The speed at which failures can occur, as demonstrated by the growth in computer viruses and Denial of Service attacks, places new demands on response and recovery planning.

The following are some cyber incidents that could occur:

- Loss of e-trading systems, which prevents buyer/seller transactions, and loss of e-commerce/B2B systems, which affects the ability to procure materials and services. Both of these can disrupt operations.
- Unauthorized modification of company trading transactions.
- Loss of critical business systems (e.g., customer service, financial, connectivity) or modification of critical decision data, which could affect both physical operations and business continuity.
- Loss of access to the Internet, telecommunications, or electric power, which can disrupt physical operations.
- Interception and/or modification of SCADA data, or the loss of a SCADA system, which affects the ability to operate a pipeline or facility (e.g., refinery, compressor station) potentially causing a loss of service.
- Release of sensitive customer information/billing information.

- Unauthorized company information posted on the Internet, including messages that are false and defamatory in an attempt to manipulate stock price.
- Hijacking and modification of company web sites.
- Interception and inappropriate use of sensitive company communications.

Gaps in Cyber Infrastructure Response and Recovery

Cyber response and recovery processes are not as mature as those developed to handle damage to physical assets. Enhancements need to be made in the areas of cyber response and recovery planning in assessing data backup policies and procedures, automation control systems design redundancy, protection of cyber systems that operate critical infrastructures, the reliability of external paths through which critical information flows, the inconsistency in how nations legally address cyber issues, and the lack of international cyber security standards.

Since company policy and procedure form the cornerstone for how a company responds to incidents, they must be kept up to date. Policies and procedures to deal with new economy cyber threats need to be developed and/or improved. Best practices in this area need to be shared to speed up the implementation of adequate cyber response and recovery processes throughout the industry.

Companies today are essentially operating within their own spheres with no previous requirement to cooperate and share information. Some companies have put in place virus-incident response plans to deal with virus attacks. And some organizations are now working to develop more sophisticated, overall cyber-incident response plans that incorporate an interdisciplinary response to intrusions (external and internal), fraud, viruses, denial of service, website hacks, etc. Companies also need to develop internal information-sharing mechanisms to receive, analyze, and disseminate incident information from internal and external sources.

Cyber Incident Response Plans are a way to provide simple, well-understood systematic procedures for responding to security-related incidents. A well thought out, direct approach to guide through many types of incidents is best. Organizing an incident handling team and selecting members is one of the first steps. Potentially the team should include personnel from different disciplines such as desktop and server support, local and wide-area telecommunications, public relations, legal, audit, and investigations.

A response plan should include information in six general areas: preparation, detection, containment, eradication, recovery, and follow-up.[3] Pre-designed reporting forms facilitate rapid communications, and an up-to-date contact list creates links to other personnel from which to obtain help or decisions. If law enforcement is going to be involved, then additional steps may be necessary to preserve evidence in a manner acceptable to the courts.

Special actions must be incorporated into these general plans to handle situations such as the following:

- Malicious Code Attacks – viruses, Trojan Horses, worms, and scripts used by hackers
- Probes and Network Mapping – probes try to gain access or information
- Hoaxes – false alarms that tie up incident response resources and spread fear, uncertainty, and doubt through the user community
- Espionage – stealing of information to subvert the interests of the organization.

[3] Incident Handling Step by Step, A Survival Guide for Computer Security Incident Handling, The SANS Institute, Version 1.5, May 1998.

The computer incident response plan must be coordinated with existing disaster recovery and/or business continuity plans. Damage from cyber security incidents may result in the activation of contingency plans to recover networks, systems, and data. These actions would occur concurrently with the ongoing incident response.

Currently, there are limited best practices that deal with cyber security. However, British Standard 7799, "The Standard for Information Security Management," has been adopted by the International Standards Organization (ISO) as ISO 17799, dealing with information security administration.

Cyber attacks can be launched from anywhere in the world. If an incident is to be successfully prosecuted, law enforcement must obtain evidence in all of the involved jurisdictions. The Department of Justice is working in several different forums, like the G8 and the European Operating Council, to establish standards for cyber crime laws and to develop contact lists through which law enforcement can obtain assistance in these other jurisdictions 24 hours a day, seven days a week. However, until most nations recognize the benefits of the new business environment, and pass laws to deal with cyber crime, it will continue to be difficult to respond, investigate, and prosecute. As an example, the author of the "ILoveYou" virus was set free because no laws existed in the Philippines at that time to make the act a crime.

Globalization, Restructuring, Political & Regulatory, and Interdependency Issues

The issues of globalization, corporate restructuring, political and regulatory uncertainty, and interdependency, as discussed previously in this report, further exacerbate consistent response and recovery planning. A recent incident of an infrastructure failure that had cascading effects was the explosion 20 miles south of Carlsbad, New Mexico, just before dawn on Saturday, August 19, 2000. The line was one of three adjacent pipelines providing natural gas to Arizona and California. Electric generation customers in those states are dependent on natural gas supplies from these lines. After the rupture, all three natural gas pipelines were shut down, and shipments to customers halted.

The initial response to the explosion was by local, state, and company officials. The Office of Pipeline Safety, National Transportation Safety Board, and Environmental Protection Agency responded based on their jurisdictions. At least six different entities were at the site with different perspectives, jurisdictions, and agendas. Initial actions at the site revolved around containment of the cause of the explosion to protect the safety of other citizens and emergency responders, and then the ensuing investigation into why the pipeline ruptured and exploded. If terrorism were suspected, then the Federal Bureau of Investigation (FBI) would also become involved.

Due to the potential impact on natural gas supply to the western states, an assessment of the impact of the pipeline outage was critical. California would be significantly impacted if the pipeline outage cascaded into a shutdown of natural gas-fired electric generation plants. The Department of Transportation requested that the Department of Energy provide an energy impact assessment.

This example brings into focus the implications of infrastructure failures at the regional and national levels. The following are issues or questions that must be considered:

- An incident can transcend an individual company and the industry itself, and it can affect other infrastructures, widespread geographic areas, and other countries.
- What supporting role should government provide to industry in developing assessments

of possible consequences that transcend an individual company, or an industry?

- Should plans be developed for simultaneous incidents such as earthquakes, cyber attack, energy supply system failures, etc., and coordinated with other infrastructures?

- Who has the authority to resolve jurisdictional disputes and cause the rapid restoration of service to mitigate the downstream consequences?

- What role should local and state governments (or the governments of affected countries) play in regional or national response and recovery operations?

- What types of information should be shared during incidents to keep everyone informed, and provide after action reports from which best practices or lessons learned can be derived?

BEST PRACTICES TO ENHANCE RESPONSE AND RECOVERY

Evaluate Optimal Models

A number of organizations and government agencies collect and disseminate information on lessons learned from emergency response and recovery activities. For example, FEMA, EPA, the Department of Transportation's Office of Pipeline Safety, the Coast Guard, the FBI's National Infrastructure Protection Office, and the Nuclear Regulatory Commission are federal agencies with relevant experience. In addition, a number of safety and emergency prevention groups serve as information clearinghouses. Examples are the Houston Ship Channel Consortium, Chemical Safety Board (which functions in a manner similar to that of the National Transportation Safety Board), and American Institute of Chemical Engineers' Center for Chemical Process Safety. It will be important to characterize the types, frequencies, and severities of incidents comparable to those that could be experienced in the oil and gas industries; determine the amount of time it took to restore service; identify the factors (if any) that inhibited quick recovery; and evaluate the associated costs. Thus, additional research needs to be done to evaluate how these clearinghouse systems work and to determine which features could best be applied to response and recovery planning, testing, and execution for the oil and natural gas industries.

Year 2000

Contingency planning for Y2K was a highly successful model of response and recovery planning and cooperation. At the national level, the government did several things to assist industry:

- Laws were passed to facilitate information sharing among companies, and to limit liability.

- Readiness reporting standards were provided.

- A national command center was established by the government to collect and collate Y2K information and disseminate it to others during the time change.

- Space was provided in the command center for key infrastructure groups to gather and monitor activities in their areas, which would improve communications and provide for faster response to problems.

Periodic Tests (Benchmarks, Tabletops, Communications)

Contingency plans exist at different levels. These levels are based on constituencies and their different roles in response and recovery. Local government, state government, industry associations, the federal government, and international entities have different jurisdictions and interests. The impact of consequences on them and their response to those impacts must be anticipated and planned for. The impacts of the new business

environment drivers, the global news market, and the timing of response versus recovery add increased complexity. These increasingly complex response and recovery environments dictate that plans be periodically tested to ensure they will manage the consequences of the emergency and reduce risk for all stakeholders. Companies also conduct periodic testing of plans to comply with regulations like the Oil Pollution Act of 1990. The benefits of testing include:

- Validation of overall adequacy of the plan
- Validation of plan assumptions
- Validation of ability of staff to execute (skills and experience)
- Identification of unexpected problems
- Identification of new issues
- Identification of plan failures
- Staff training.

Tests should be conducted at appropriate times. A mature testing process includes both scheduled and unannounced tests. Successful unannounced tests are the best indicators of a company's capability. There are different types of tests that can be done to test the adequacy of plans:

- **Benchmarks.** A benchmark is a test where standard data types are collected over time for comparison against either an industry standard (benchmark) or against a collection of similar companies. This is a good way to see if standards are being met, such as government regulations, quality, or safety targets, etc. In a test, benchmarks could be response time, actions taken, reports filed on time, time to recover services, number of personnel who didn't respond to pages or other notification, etc.
- **Tabletop Exercises.** A tabletop is a more realistic test of a plan where it is impossible to use the actual physical assets to simulate the emergency. Scenarios are developed to create situations that exercise the response and recovery team member's roles, communications, logistics, and command and control. Tabletops are very useful in getting different stakeholders together to test multi-level integrated response and recovery plans.
- **Communications.** A communications test may be as simple as testing a calling tree or employee notification process to ensure that critical staff can be reached. Or it could be to see if a request for mutual aid could be executed effectively. It could be to test a media relation's plan with scenarios for them to respond to and conduct simulated briefings to the media. Or it could be a technical test of backup telecommunications.
- **Cyber Exercises/Tests.** Disaster recovery tests are the traditional type of testing done. Tests can include:
  - Telecommunications tests
  - Backup and recovery tests for data, systems, and applications
  - Hot site (duplicate environment)
  - Tabletop exercises to test command and control
  - Security tests to identify cyber vulnerabilities, or to test incident response plans.

  In addition to the benefits listed above, the benefits of cyber testing permit identification of missing general or special purpose computing equipment, wrong network protocols or missing protocol capabilities, missing circuits to key network nodes, wrong cables, missing data or data feeds, missing applications, and so forth. All of these can easily defeat testing in a complex computing environment of hardware, microcode, software, data, applications, networks, and people.
- **Functional Exercise/Test.** When plans are large and complex, it may be necessary to break them

into manageable pieces for testing. This can be accomplished by testing specific functions separately (e.g., incident command and control, decision making, communications, etc.).

As response and recovery plans become more sophisticated, the ability to adequately test these plans is increasingly difficult. A single company may not be able to test their ability to handle "all"consequences. It may be necessary in the new business environment for groups of companies to perform integrated tests together.

Information Sharing

A formal industry-wide information-sharing mechanism should be adopted to enhance the flow of information during an incident to all stakeholders. The sheer size and complexity of the oil and natural gas industries, and the need to partner with other companies, infrastructures, and local, state, and federal governments to deal with wide ranging consequences require that all parties be kept up to date during the life of an incident. An information-sharing mechanism could:

- Serve as a formal focal point for our sector to collect and distribute information during an incident.
- Collect incident and post mortem information for analysis.
- Provide information to all stakeholders: federal agencies, state and local governments, and the On Scene Commander of the incident.
- Facilitate the development and maintenance of a "Yellow Pages" directory of critical skills, materials, services, and other response and recovery resources that could be shared by companies during an emergency.
- Provide clarifications and supplementary guidance that companies could use to help them understand and address response and recovery planning issues.
- Disseminate information on response and recovery training, outreach programs, and other topics from government and industry organizations.
- Provide feedback on response and recovery planning best practices and benchmarks from inside and outside the sector to all stakeholders.

FINDINGS AND CONCLUSIONS

- The oil and natural gas industries are well positioned to handle physical infrastructure disruptions.
- The oil and natural gas industries rely on information technology and telecommunications to operate physical infrastructures, trading systems, and general business processes. The consequences of this reliance pose additional challenges to effective response and recovery planning.
- Cyber response and recovery capabilities and processes are not as mature as those developed to handle physical incidents. Companies need to review and update response and recovery plans to ensure they address the cyber dimension.
- Information in the cyber dimension is a critical resource and must be recovered. Without the information, the infrastructure recovery is meaningless. Cyber response and recovery plans should be grounded on effective data backup and recovery policies and procedures.
- Companies need to ensure that periodic exercises and tests are conducted to validate response and recovery plans for critical infrastructure assets.
- The new business environment dictates that companies include key stakeholders, such as

business partners, suppliers, customers, and representatives from local and state governments in response and recovery tests and exercises.

- Companies need an effective internal information-sharing mechanism to receive, analyze, and disseminate incident information to and from internal and external sources, including law enforcement to enhance response and recovery.

- Timely and actionable information is the key to an effective response to threats or incidents, as well as to successful recovery activities.

- Companies need to review their mutual aid agreements to ensure they are still effective in the new business environment.

- In the new business environment, the potential for cyber and physical incidents to cascade into regional, national, and international impacts is greater. Industry should work with government to develop regional response and recovery plans, including periodic testing and exercises, to provide mechanisms to deal with these larger impacts.

- When infrastructure disruptions occur, the roles and responsibilities within local, state, and federal governments often conflict. These conflicts of interest regarding jurisdiction impede timely restoration of service to industry customers, and can also inhibit future infrastructure protection.

- The oil and natural gas industries in partnership with government needs to continuously study other industry and government response and recovery models to enhance best practices for response and recovery planning and incident management.

- To better protect the critical infrastructures of the United States, the federal government should:

  – Clarify the response and recovery roles of the various federal and state agencies, including the Federal Emergency Management Agency.

  – Work with industry and other government entities to identify new response and recovery processes and improve awareness of each other's capabilities in the area.

  – Assist in understanding interdependencies with other critical infrastructures.

  – Coordinate with all affected parties to provide accurate and timely information about incidents.

  – Develop a process that enhances response and recovery by allowing temporary waivers in the face of constraining regulations to address critical infrastructure impacts.

  – Review the actions taken to address the Y2K issue and build on this successful model to address concerns raised in the critical infrastructure protection area.

CHAPTER 5

Information Sharing and Sector Coordination

The oil and gas industries have long recognized the need for security of physical assets. As a result of recognizing this need, the industries have developed effective systems to protect critical physical infrastructure. The advent of the information technology age with its assorted electronic tools and systems requires an extension of protection to critical electronic infrastructure. There is a high level of interconnectivity of electronic systems, both with physical systems and other electronic systems. Along with the speed with which information is transferred, it is apparent that a system that provides early warning of emerging situations that may compromise electronic infrastructure security is desirable and may, in fact, be essential. One positive approach to providing early warning is to use an industries-wide information-sharing mechanism.

In order to better facilitate information flow in the industries, there appears to be the need for a central focal point. This focal point could be either an individual or an organization that would be charged with coordinating information flow within the industries and would be designated as sector coordinator.

INFORMATION SHARING

The study of vulnerabilities and threats in the oil and natural gas industries determined that the industries' dependence on information technology and telecommunications, including e-commerce and supervisory control and data acquisition (SCADA) systems, to manage business internally and externally, are areas where a catastrophic event or failure could have a significant negative impact on all or part of the economy. This study determined in part:

- Competitive pressures can often lead to the use of immature technologies and can introduce significant vulnerabilities to enterprises and the infrastructure.
- The oil and natural gas industries are faced with a continuous stream of patches and fixes to correct hardware and software security defects.
- Failure of joint or shared use systems for e-commerce not only has a negative impact on a member of the shared service, but also can cascade throughout the infrastructure creating a significant vulnerability.
- The ability to go back to old manual methods is extremely difficult, as oil and natural gas companies become reliant on these information technology and telecommunication systems. Because of the change in organization, the workforce is no longer as experienced or as skilled as before and it lacks the ability to operate systems without cyber tools, thereby limiting the capability to return to older manual methods.
- A failure in the telecommunications infrastructure will create significant impacts to the oil and natural gas infrastructures because of local and wide-area networks interconnecting new economy systems.
- Systems are vulnerable to externally initiated events because it is no longer necessary to be on the premises to launch an attack, or to create an interruption.

- Rogue nations, terrorists, or other enemies are developing cyber capabilities to attack cyber infrastructures.

- The integration of information technology and telecommunications into business is creating a critical interdependence between infrastructures, i.e., banking and finance, power, water, oil and natural gas, transportation, telecommunications, and information technology.

Experience has shown that early warning of incidents or new vulnerabilities affecting information technology systems is critical to system protection. Therefore, creation of, and active participation in, an oil and natural gas information sharing and analysis center (ISAC) is paramount to the protection of this infrastructure.

The oil and natural gas industries have developed several forums for information sharing that provide individual companies with value today. Formal mechanisms for coordination and information dissemination exist through trade advocacy groups (regional, national, and international), vendor expositions, conferences, workshops, and training programs. However, these information-sharing mechanisms are reactive in nature and do not provide the critical insights into real-time information that can prove critical to protecting industry infrastructures. While physical security issues benefit from information sharing, the speed at which cyber incidents spread dictates the need for real-time information sharing.

Within the oil and natural gas industries, companies differ greatly in size, from global multinationals to sole proprietors. Many companies do not have an adequate IT security staff, and smaller companies may have none. Many of the smaller companies are doing contract work for the multi-nationals and access their information systems. Companies throughout the infrastructure are not receiving and acting on vulnerability information in a timely manner. Having access to an ISAC at a reasonable cost would provide all companies in the sector with timely warnings and solutions that they otherwise would not get.

The oil and natural gas, water supply, and electric power sectors are dependent on SCADA systems, which are used to operate physical infrastructures and refining processes. These systems increasingly rely on open architecture and the Internet to perform their critical functions. These open systems may be corrupted by external sources, which could cause disruption and great cost to the industry. Therefore, vulnerabilities in these systems will benefit from information sharing within the industries and with the vendors of such systems.

As pointed out in Chapter 4 discussions of response and recovery, information sharing during incidents is critical to ensure smooth response and restoration of critical services. The sheer size and complexity of the oil and natural gas industries and the need to partner with other stakeholders to deal with wide-ranging consequences require that all parties be kept up to date during the life of an incident.

Companies today receive threat warnings from multiple sources. Often these warnings are on the basis of personal subscription, not centrally coordinated, or on a timely basis. For example, the "Anna Kournikova" virus resulted in multiple messages warning companies about this virus, which in actuality slowed down e-mail systems and caused a larger impact on business operations than the virus itself. If an industry information-sharing mechanism existed, one warning and the solution could have been transmitted to ISAC members ahead of the spread of the virus, minimizing the impact on corporations.

In addition to viruses, denial of service attacks, hackers, internal and external fraud, human error, etc., can seriously disrupt business operations at great costs. This study found no other real solutions to adequately deal with the myriad cyber

attacks without such an information-sharing mechanism.

INFORMATION SHARING STATUS OF OTHER CRITICAL INFRASTRUCTURES

In addition to the oil and natural gas industries sector, the federal government has identified seven other critical infrastructures. While each sector has some characteristics that are in common, each has its own unique set of characteristics. Consequently, it is not surprising that the various sectors are addressing the issue of information sharing in different ways. For example, there are three general models for implementing an information-sharing mechanism: reliance on industry staff, use of an industry-directed service provider, or a hybrid government/industry management.

The ISAC approach is being pursued by four of the sectors: banking and finance, information technology, electric power, and transportation. One sector is following another information-sharing path: telecommunications. The remaining three sectors are currently in the early stages of addressing their critical infrastructure protection needs: water supply, emergency services, and government services.

Banking and Finance Sector

The Financial Services Information Sharing and Analysis Center (FS/ISAC) became operational in October 1999. Predictive Systems Inc., an industry-directed service provider, operates the FS/ISAC. The banking and finance sector established the FS/ISAC as a limited liability corporation (LLC) which owns the sector's analysis processes and information submitted by members. An elected Board of Managers who is responsible for the operating rules and guidelines for the ISAC governs the LLC. The FS/ISAC receives information from the government but does not share information back.

There are several desired attributes from this model such as: the use of a limited liability corporation structure for the ISAC; the availability of real-time IT threat and vulnerability information; anonymous posting of incident data; the availability of IT solutions from the ISAC; the sending of tailored and prioritized alerts; cost-effective operations; and strategic partnerships with IT vendors to broaden data sources.

Information Technology Sector

The Information Technology Association of America (ITAA) is the sector coordinator for the information technology sector. As of early May 2001, the ITAA has announced that it is forming an operational ISAC. Its purpose will be to facilitate the timely sharing of non-proprietary information concerning threats of cyber attacks (alerts), actual attacks (analysis and trending), and countermeasures to attacks. The ISAC will serve as the sector focal point for coordination, cooperation, and information sharing. ITAA also has chosen to use an industry-directed service provider to operate their ISAC.

Today's businesses are very dependent on information technology. Since there continues to be exploitation of IT vulnerabilities, this ISAC could play a key role in cross-sector information sharing.

Electric Power Sector

The North American Electric Reliability Council (NERC) is the sector coordinator for the electric power sector. They are currently implementing an indication and warnings system with the National Infrastructure Protection Center (NIPC) to serve as their information-sharing mechanism. NIPC serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.

The electric power sector is providing the federal government with information about malicious

incidents that can then be shared with the electric power industry. The indication and warning system being adopted by the electric power industry provides a valuable linkage with the government. Certain industry staff have security clearances, and are able to receive directly from NIPC classified threat and vulnerability information that ordinarily could not be shared. They can then work with the government to declassify such information and share it in a valuable format to other non-cleared industry staff.

Telecommunications Sector

The National Coordinating Center for Telecommunications–Information Sharing and Analysis Center (NCC/ISAC) has evolved from an entity that provided indications, analysis, and warning (IAW) capabilities into one that now operates as an information-sharing mechanism. They are developing the NCC/ISAC to facilitate voluntary collaboration and information sharing among its members. The scope includes a broad range of vulnerabilities and threats with potential to affect the telecommunications sector. Information is shared on a non-attributable basis. The strength of the NCC information-sharing mechanism is its ability to pull major industry players into a room to discuss infrastructure activities impacting their industry.

Because of the dependencies on telecommunications technology, this information-sharing mechanism could play a key role in cross sector information sharing.

INFORMATION SHARING REQUIREMENTS FOR THE OIL AND NATURAL GAS INDUSTRIES

The National Petroleum Council examined information-sharing mechanisms within the oil and natural gas industries, in other critical infrastructures, and from other industries. Specific successful information sharing models such as the Centers for Disease Control were examined to glean desired ISAC attributes and criteria. The NPC determined that an oil and natural gas sector ISAC should be capable of the following:

- Providing access to the broadest range of threat, vulnerability, and incident data involving IT hardware and software products, SCADA systems, and physical assets.
- Providing data acquired from the broadest range of global sources to include technology vendors, Internet sources, industry participants, other ISACs, local, state, national, and foreign governments, businesses, etc.
- Providing global capabilities to identify, analyze, and disseminate information on threats and vulnerabilities in real time.
- Analyzing high volumes of data, using a combination of automated and human processes.
- Prioritizing cyber incidents and providing members with timely and relevant alerts and solutions.
- Providing members a choice to remain anonymous when reporting incident information to the ISAC. Membership in the ISAC can also remain anonymous.
- Providing a single repository for access to threat, vulnerability, and incident identification and solutions.
- Providing demonstrated experience in operating ISACs.
- Operating in a cost-effective manner, providing greater value than the cost of joining.

In addition to the requirements listed above, it is possible that an arrangement can be made with NIPC to share classified threat information with designated personnel in the oil and natural gas sector. For example, as previously noted, in the electric power sector certain industry staff have security clearances, and are able to receive directly from NIPC classified threat and vulnerability

information that ordinarily could not be shared. They can then work with the government to declassify such information and share it in a valuable format to other non-cleared industry staff.

ISSUES AND CHALLENGES FOR INFORMATION SHARING

Information sharing is appropriate for the oil and natural gas industries to leverage their internal knowledge base at an individual company level, within the industry, with other industries, and with government. Information sharing can assist in better understanding vulnerabilities and threats along with mitigating risk and improving response and recovery planning. However, obstacles related to information sharing must be addressed in order to maximize the benefits from information sharing. These obstacles relate to issues with sharing within the industry, industry sharing with government, and government sharing with industry. Each of these obstacles is discussed below.

Issues and Challenges for Sharing within Industry

As previously discussed, information sharing currently exists within the oil and natural gas industries. Information sharing exists between companies, from trade associations, and research organizations. There are challenges, however, that impede some desired information from being shared. These challenges must be addressed so that effective information sharing can occur. These challenges include:

- **Size and Complexity of the Oil and Natural Gas Industries.** The oil and natural gas industries are comprised of many segmented and diverse companies and associations, making it difficult to categorize and coordinate these industries. Some companies choose strategically to own and operate assets while others perform a market function of buying and/or selling commodity products without the ownership of assets. Still others are developing energy-related financial products that are becoming increasingly essential to the seamless operation of the infrastructure. It is difficult to reach out to all these diverse industry components.

- **Liability Arising from Participation in an ISAC.**[1] There are many potential sources for liability stemming from the formation and operation of an ISAC. However, most of the potential liability can be minimized through an effective allocation of the risks through several contractual arrangements, such as the ISAC membership agreement, service agreement with ISAC provider, and ISAC membership rules.

- **Antitrust Laws and Information Sharing.**[2] Information sharing among competitors must be consistent with federal and state antitrust laws. The U.S. Department of Justice (DOJ) has stated that it would not challenge a proposal by the Electric Power Research Institute (EPRI) to share cyber vulnerability and threat information within the electric power industry. This action supports the belief that DOJ will not act under the antitrust laws against ISACs that are legitimately focused on cyber security. The risk of antitrust liability for information sharing can be minimized by obtaining a business review letter from DOJ for the oil and natural gas industries ISAC.

Issues and Challenges for Industry Sharing with Government

Although much information from industry is shared with government, several obstacles currently impede additional information sharing. These obstacles must be addressed so that effective information sharing can occur. Critical infrastructure protection has always been treated as a private/public partnership. For this partnership to

[1] Potential liability concerns arising from participation in an ISAC are more fully discussed in Chapter 6 of this report.

[2] Potential antitrust concerns arising from participation in an ISAC are more fully discussed in Chapter 6 of this report.

be truly effective, the information sharing obstacles need to be resolved. These obstacles include:

- **Protection for Companies' Sensitive Information.** Under the Freedom of Information Act, the government must publicly release certain types of information when requested. Without the necessary protection that prohibits release of sensitive business information, companies are reluctant to voluntarily share information with government. Statutory changes in the law need to be addressed to remove this obstacle.

- **Role of State and Local Governments.** State and local governments play important roles for the oil and natural gas industries. Local governments are the first responders to incidents and assist in response and recovery. State governments play an important role in safety, environmental, and emergency preparedness. Many states have freedom of information type laws. Therefore, industry may be reluctant to share information that could become public. The relationship between industry and the federal, state, and local governments must be clearly defined. The government can provide additional assistance to industry if industry shares their requirements and needs.

- **Year 2000 Readiness and Responsibility Act.** During the Year 2000 rollover there was much concern about the liability of collecting and sharing information. This information was important to all critical infrastructures to assess the state of the infrastructures and share solutions and expertise. The Y2K Readiness and Responsibility Act (the "Y2K Act") was designed to reduce uncertainty regarding what legal standards apply to Year 2000 disputes, and thereby reduce frivolous litigation and encourage remediation. The Y2K Act helped to establish uniform, national legal standards and liability limitations governing lawsuits arising from actual or potential Year 2000 failures. Something similar is needed before the full benefits of sharing information regarding critical infrastructure protection can be realized.

Issues and Challenges for Government Sharing with Industry

The federal government has a key role to play in sharing information with the oil and natural gas industries. Leveraging information available in the federal government, whether practices employed or intelligence known, can assist companies in better understanding their risk exposure and lead them to better understand what appropriate mitigation options to undertake.

Several obstacles currently prevent the government from sharing additional information with industry. Perhaps the largest difficulty that the government faces in this regard is sharing classified and unclassified intelligence and threat information they have collected with industry. The obstacles the government faces with sharing information with industry include:

- **Impact of Classification on Information Sharing.** An important element of the federal government's case for critical infrastructure protection is founded on federal intelligence information. However, classified information retained by the government, and not shared with industry, provides limited value to the oil and natural gas industries. The "declassified" form of federal intelligence often provides little meaning and value. There are various incidents and warning information provided to the sector including alerts from the NIPC, the FBI, and the U.S. Department of Transportation. Often these alerts are so "watered down" as to be non-actionable. Industry personnel who have obtained government security clearances do benefit from participation in government-sponsored seminars on critical infrastructure protection. However, by virtue of this clearance they are prohibited from sharing the knowledge gained within their company, much less with other industry participants.

- **Implications for Information Sharing with Foreign Affiliates.** Foreign-owned and multinational corporations are another obstacle to overcome. A company's loyalty usually exists to its shareholders and not the government. But this may not be the case for foreign-owned businesses. Some businesses have headquarters in other countries and hence loyalties to these countries. Deciding what types of information and under what circumstances to share are difficult issues. U.S. firms often partner with non-U.S. firms that may share access with company systems, creating potential vulnerabilities to the U.S. infrastructure.

INFORMATION SHARING RECOMMENDATIONS

The National Petroleum Council recommends the development and implementation of an oil and natural gas ISAC. Such an ISAC would help mitigate the sector's collective risk considering its dependency on IT, telecommunications, and SCADA systems. Additionally, because of the convergence of oil, natural gas, and electric power into an energy industry, these industries can no longer be examined independently. Most energy companies have activities in two or more of these energy commodities. It is recommended that after the oil and natural gas industries ISAC is operational, consideration should be given to include other entities, as interrelationships become apparent.

While there are issues and challenges to some types of information sharing, they do not prohibit the development of the ISAC. Initially, information will not be shared with government until current barriers are removed. As more of these barriers are removed, the value of the ISAC will increase even further.

It is recommended that an arrangement be initiated with government to permit certain industry personnel to obtain national security clearances in order to access classified threat information. Access to such classified information would enhance vulnerability assessment for the sector.

In order to facilitate information sharing without an encumbrance of the antitrust legislation, it is recommended that the ISAC obtain a business review letter from DOJ to allow information sharing regarding cyber security.

The industry-directed service provider model is recommended as the most efficient and appropriate for the oil and natural gas sector. The "information sharing requirements" of an ISAC, described earlier in this chapter, should be utilized in selecting the best service provider. Information technology and telecommunications vulnerabilities should be the immediate focus, but inclusion of physical vulnerabilities and threat information should be included in the evolution of the ISAC. The National Petroleum Council found that some energy companies do not receive enough of this crucial information, and some companies may not receive any at all. Additionally some companies may not have a physical or IT security staff to act on this crucial information. A cost-effective ISAC would permit those companies access to timely vulnerability and threat information along with solutions.

In determining the structure and operating procedures of an ISAC, the NPC recommends that an industry board be established to investigate, develop, and implement an appropriate ISAC for the sector. This board would address issues such as membership, legal structure, costs, selection of a service provider, etc.

SECTOR COORDINATION

Purpose

The National Petroleum Council is a federal advisory committee that provides advice, information, and recommendations on matters relating to oil and natural gas and their industries

solely at the request of the Secretary of Energy. As such, the NPC accepted an interim role as sector coordinator to lead the oil and natural gas sector in responding to Presidential Decision Directive 63. In the request letter, the Secretary of Energy asked, "At the conclusion of your work, I would like your advice on the permanent role of the Sector Coordinator, and your recommendation on how that person or organization should be identified."

Discussion

Information that relates to the roles and responsibilities of the sector coordinators are described in several documents generated by the government on critical infrastructure protection. They are the Presidential Commission on Critical Infrastructure Protection,[3] and an unclassified white paper on Presidential Decision Directive 63.[4] The goals for each sector listed in Presidential Decision Directive 63 include:

- Assess the vulnerabilities of the sector to cyber or physical attacks.
- Recommend a plan to eliminate significant vulnerabilities.
- Propose a system for identifying and preventing attempted major attacks.
- Develop a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstitute minimum essential capabilities in the aftermath of an attack.
- Ensure that all plans and actions take into consideration the needs, activities, and responsibilities of state and local governments and first responders.
- Strongly encourage creating a private-sector ISAC. (Design and functions will be determined by the private sector.)

Three main issues present themselves in providing sector coordination: the ability of the designated group or individual to provide leadership and ongoing day-to-day interaction with various stakeholders; access to administrative staff; and funding to support sector activities.

Through interviews with current sector coordinators, it was apparent that each sector has taken a different approach to achieving critical infrastructure protection goals in response to the presidential decision directive and input from their industry members. Each sector coordinator is providing leadership, staffing, and funding in different ways. Therefore it is up to the oil and natural gas industries to decide how best to provide this critical leadership and coordination function. The roles and responsibilities of the sector coordinator will evolve over time as infrastructure protection goals and industry's approach to security mature. The initial commitment to initiate and implement the recommendations of this report on behalf of the industries must not be underestimated.

SECTOR COORDINATION RECOMMENDATIONS

Roles and Responsibilities for the Oil and Natural Gas Sector Coordinator

The National Petroleum Council has identified the following sector coordinator roles and responsibilities that are appropriate for the oil and natural gas industries:

- Provide oil and natural gas sector leadership on critical infrastructure protection matters, such as facilitating establishment of a sector ISAC and participating in its management.

[3] *Critical Foundations, Protecting America's Infrastructures.* The Report of the President's Commission on Critical Infrastructure Protection. October 13, 1997.

[4] White Paper – The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998.

- Be the primary liaison for the sector on critical infrastructure protection matters with industry, Department of Energy, other critical infrastructure protection sectors, the executive and legislative branches of government, media, and state and local government entities.

- Define the financial structure for operation of the office of the sector coordinator.

- Establish working groups from the sector to address pertinent critical infrastructure protection issues and industry goals such as training needs, awareness programs, and identification of sector R&D needs.

- Encourage sector industry components to perform periodic, quantitative risk assessments of information and telecommunication systems and physical security to enhance awareness of new vulnerabilities.

Selection of a Sector Coordinator

The National Petroleum Council recommends that the sector coordinator be designated by the governing body of the oil and natural gas industries ISAC.

FINDINGS AND CONCLUSIONS

Information Sharing

- Experience has shown that early warning of incidents or new vulnerabilities affecting information technology systems is critical to system protection.

- The oil and natural gas industries have several forums in which information is shared, but there is no designated information-sharing mechanism that focuses on cyber aspects of critical infrastructure protection.

- Information sharing through an ISAC has proven to be a valuable approach in mitigation of cyber vulnerabilities and threats.

- The oil and natural gas industries would benefit from the creation of an ISAC. From the three models in use throughout the critical infrastructures, it is recommended that an industry-directed service provider operate the ISAC for the oil and natural gas industries.

- The industry dependence on information technology and telecommunications pose immediate vulnerabilities. Therefore the recommended initial focus for the ISAC should be information technology and telecommunications.

- Many companies in the sector do not have an adequate IT security staff to support their systems, and smaller companies may have none. Participation in an ISAC would provide a cost-effective method for them to access timely data regarding cyber security incidents and solutions.

- Industry access to classified threat information would further enhance the protection of the oil and natural gas infrastructures. An arrangement should be initiated with government to permit certain industry personnel to obtain national clearances in order to have access to classified information.

- There is a convergence within the oil, natural gas, and electric power industries in the marketplace with companies having activities in two or more of these commodities. Future consideration should be given to offering the opportunity for all companies in the energy business to join the oil and natural gas industries ISAC.

- SCADA systems are used in the oil and natural gas, electric power, and water supply industries. Therefore, future consideration should be given for private water supply companies to join the oil and natural gas industries ISAC.

- It appears that a properly structured industry information-sharing mechanism can operate within existing law.

- The oil and natural gas industries are sensitive to the government's antitrust concerns. A business review letter addressing antitrust concerns on information sharing should be obtained from the U.S. Department of Justice. The preferred long-term solution would be new legislation.
- To facilitate information sharing by industry with government, legislative action is needed to provide relief from liability and the Freedom of Information Act.
- The NPC has identified ISAC requirements and selection criteria to facilitate information sharing within the oil and natural gas industries, which would serve as the basis for selecting a vendor.
- The governing body for the oil and natural gas industries ISAC should have balanced representation from all segments of the industries.

Sector Coordination

- Sector coordination is a critical component to implementing an effective critical infrastructure protection program providing overall leadership and a point of contact to deal with day-to-day infrastructure protection issues.
- Currently no organization represents all segments of the oil and natural gas industries. The governing body of the sector ISAC is the logical entity to provide a neutral forum for sector coordination issues.
- It is recommended that the Secretary of Energy formally acknowledge the designee of the governing body of the oil and natural gas industries ISAC as the sector coordinator, fulfilling the responsibilities of Presidential Decision Directive 63.

CHAPTER 6

Legal and Regulatory Issues Related to Information Sharing

It is well accepted that existing legal and regulatory systems influence decisions to act or to refrain from action. It is equally clear that certain laws and regulations enacted for one purpose can have unintended consequences that are completely unrelated to that purpose. Any nationwide or international effort to secure critical infrastructure must take into account how existing laws and regulations may facilitate or impede those efforts. This chapter addresses the relevant laws and regulations that affect oil and natural gas industries critical infrastructure protection collaborative efforts (information sharing). Legal mechanisms that exist or could be put in place to encourage private-sector voluntary disclosure and to facilitate governmental sharing of critical infrastructure protection information are discussed below. Finally, this chapter discusses examples of information-sharing systems already in place for dealing with local and global problems that could serve as models for the recommendations made in this report.

For purposes of this analysis of existing laws, it is assumed that: (a) voluntary, rather than mandatory, disclosure of information to facilitate infrastructure assurance is desired[1]; (b) consensus exists or can be reached on what should be disclosed, to whom it should be disclosed, and when disclosure should occur; (c) commercial and political obstacles to voluntary disclosure (e.g., indifference or antipathy toward business rivals) can be overcome; and (d) technology exists or will be developed that will ensure the security of the information that is disclosed.

Because existing laws and regulations could hinder the voluntary participation of industry, it is crucial to determine what legal and regulatory changes may be required in order to maximize the incentives of participants in the industry to share information—beyond the mutual objective of a safer, more secure infrastructure. This chapter discusses existing legal and regulatory concerns and recommends some regulatory changes and procedural adjustments that, although general, would help the private sector with exchanging information on common vulnerabilities, threats, solutions, best practices, and security breaches and their resolutions.

LEGAL OBSTACLES TO INFORMATION DISCLOSURE AND SHARING

As mentioned previously in this report, any private-sector participant in a critical infrastructure protection information-sharing scheme faces two distinct types of legal obstacles to information sharing: those that arise when the information is to be shared solely within the participant's industry, and those that arise when information will additionally be shared with government agencies or entities. Generally speaking, the chief concerns raised by companies over information sharing within a particular industry center around antitrust infringement, the protection of confidential information, and the potential for liability resulting from a breach of contract or a transgression of state tort law. Information sharing with the federal government

[1] Numerous additional legal issues would be raised if disclosures were not voluntary but were required by the United States government or another authority. These include, but are not limited to, constitutional issues involving the fourth and fifth amendments. These issues are beyond the scope of this chapter. To date, no critical infrastructure information-sharing scheme has contemplated such draconian requirements for its participants.

raises similar concerns, but also adds an inherent inability to control how information provided to the government is disseminated or used. It is possible to minimize these concerns, however, by addressing the legal obstacles to information sharing and devising strategies for overcoming or reducing them. The legal obstacles to private- and public-sector information sharing and how to minimize their risks are addressed below.

Legal Issues Related to Information Sharing within the Sector

Any program aimed at promoting cooperation among industry participants must take into account how certain laws will affect the ability and incentive of each industry to share information. It is first necessary to determine the legality of a proposed information-sharing program within the industries, and whether prospective members could face liability for organizing and operating such a cooperative program.

It is worth noting that these issues are related to, but separate from, the obligations imposed on program participants as conditions for membership, including for example, whether participants will owe a duty to disclose and share information, to whom such duty is owed, and the legal consequences of failing to perform that duty. These issues are important, and should be carefully addressed in the membership agreement for any information-sharing program. The discussion below, however, addresses more generally how programs involving the disclosure of information among the private sector could subject participants to certain risks.

- **Industry-Wide Information Sharing and Antitrust Laws.** Exchange of information, which is largely operational in nature, has never been seriously questioned under antitrust laws. As the scope of information to be exchanged expands, however, companies will need to be mindful of the antitrust risks of exchanging with competitors, information from which their competitive situations and plans might be ascertained.

  Recently, the Electric Power Research Institute (EPRI) requested a business review letter from the U.S. Department of Justice (DOJ) with respect to a proposed information exchange designed to enhance critical infrastructure security against cyber-threats.[2] In response to EPRI's request, DOJ indicated that it would not take any enforcement action against the proposed information exchange. DOJ concluded that "all information exchanged will relate directly to physical and cyber-security" and that "no company specific competitively sensitive information i.e. prices, capacity or future plans, will be exchanged."

  The newly proposed IT/ISAC has recently sought a business review letter from DOJ. Although an antitrust exemption for critical infrastructure protection collaboration and information sharing would be the most certain way to avoid antitrust liability, such an exemption requires Congressional action, which could be months, if not years, away. In the meantime, seeking a business review letter regarding any proposed information exchange related to cybersecurity would be a prudent course for the oil and natural gas industries to follow.

- **Information Collection/Sharing and Privacy.** The decision by a company to undertake close monitoring of its computer networks, including the actions of those who access them, could create a potential for liability. If, for example, a company determined that a visitor to its website was attempting to penetrate its firewalls during such visits, it would conceivably want to share this information with other companies in its critical infrastructure

[2] Under DOJ's Business Review Procedures (28 C.F.R. 50.6) a firm describes proposed business activities to the Antitrust Division and receives a letter stating whether the Division would challenge the actions as a violation of the federal antitrust laws.

protection program, including any personal information that the visitor wittingly or unwittingly gave to the company during his visits. The liability for such action arises from the fact that in some jurisdictions the public disclosure of private facts (even if true) about an individual, where such disclosure is objectionable to a reasonable person, constitutes a common law tort. Multinational companies must also be concerned about privacy laws in the countries within which they operate. In the United States, where the disclosure to an ISAC may relate to a matter of public interest, as could arguably be the case with disclosure of information relating to threats to critical infrastructure, First Amendment and other protections may apply to prevent liability from attaching to information collection activities.

The reactions of third parties to network monitoring are not the only ones worthy of consideration. Though it need not be a requirement for membership, a company that joins an information-sharing program may be inspired to take a more aggressive approach in monitoring the network activities of its employees. Generally speaking, companies should always inform employees of the company policy for monitoring network activity. Special care should be taken in the event that a policy will be changed (especially if monitoring is to increase) to ensure that proper notification is made and consent received.

The consequences for failure to notify employees about network monitoring can be significant. A number of state and federal laws have been interpreted by some to require notice and/or consent before certain monitoring of employee communications may take place. Bills introduced in Congress in July 2000 would have cleared all uncertainty on this issue by requiring employee notification prior to any type of electronic monitoring.[3] It does not appear to be Congress' intention to prevent electronic monitoring outright; however, it would behoove any company that already undertakes or is considering to undertake employee monitoring to have in place a comprehensive policy for notification and consent, which can often be achieved by means of an employment contract or amendment thereto.

The European Union (EU) Privacy Directive outlines the types of personal information that qualify for privacy protection, and prohibits the transfer of personal data to non-EU countries that do not provide adequate levels of privacy protection. The U.S. government has negotiated a "safe harbor" arrangement with the EU, which creates the presumption for participating U.S. companies that such companies provide adequate levels of privacy protection if they comply with specific principles regarding the use, disclosure to third parties, and access to personal information. Similar regulations in other countries could impact the collection and sharing of personal information by any private-sector participant in a critical infrastructure protection information-sharing scheme.

- **Information Use and Defamation.** The prospect that the member of an information-sharing group might face liability for charges of defamation is remote, but it is a possibility that should be discussed nonetheless. Defamation, under common law, requires a disclosure to a third party of information that would harm the reputation of an identified person. This rather broad definition has been narrowed in recent years by the Supreme Court, which has sought to give greater weight to the First Amendment's guarantees of freedom of speech and press. Charges of defamation could still occur, however, if the member of an information-sharing group disclosed certain harmful information about a person, a company, or the product of a company, and that information later turned out to be untrue. Assuming the party was able to show some injury, the

[3] The companion bills were Senator Charles Schumer's S. 2928, and Representative Charles Canady's H. 4908.

member (or perhaps the entire group) could face liability.

To avoid this potential risk, the information-sharing group should ensure that it always has a good faith basis to issue derogatory reports about a particular person, company, or product. Information of this kind should only be disseminated to protect or warn other member companies about the potential harm that could result. There is, in fact, a qualified privilege that allows for the publication of defamatory statements when acting to protect the interests of another or of a group that shares common interests. Although this is not an absolute privilege or defense, it could limit a member company's liability considerably.

- **Disclosure of Privileged or Confidential Information.** A somewhat tangential concern raised by the prospect of increased private-sector disclosure of various types of information is the potential waiver of privilege that may occur as a consequence of any such disclosure. Disclosure of otherwise privileged information developed at the direction of a corporation and its attorneys may waive privilege with respect to the information itself and information on the same subject matter. Under current law, the disclosure of any privileged communication with respect to a given matter waives the privilege for all communications related to the same subject matter. Thus, there may be a reluctance to voluntarily disclose such information without an agreement among the parties to an information-sharing group, or between the group and the federal government, that privilege is not waived through disclosure of information for infrastructure security purposes.

  It also bears noting that private-sector participants are unlikely to disclose confidential information, even where important to the protection of the infrastructure, without legal guarantees that the confidential nature of such information will be maintained. Disclosure of infrastructure vulnerabilities could create potential liability for private-sector participants if such vulnerabilities cause harm to third parties. In addition, disclosure of such vulnerabilities could impact a private-sector participant's business reputation or affect investor confidence. Concerns in the foregoing areas are heightened for private-sector participants if information concerning infrastructure security is shared with the government sector, and will be discussed in detail below. In cases where confidential information is to be shared only with members of one's industry, one way to protect confidentiality is through the membership agreement provisions that will bind the members of the information-sharing group and impose penalties for violation of the agreement.

- **Failure to Disclose or Use Information.** Prospective participants in an information-sharing program may also be deterred by the possibility of incurring liability for failing to disclose, or alternately, failing to use information on critical infrastructure attacks. The theory of liability in the former case is based on the principle that a member in an information-sharing group has an obligation (and not an option) to share information about attacks with other members of the group. If this duty is not explicitly set forth in the membership agreement, however, then it is unlikely that such a duty would be implied under federal or state law.

  Liability in the latter situation could be triggered if a company is aware of a particular threat but does not take any actions to defend against it, and falls victim to attack. Should such an event occur and be fully discovered by a third party, such as a customer or shareholder of the company, it is foreseeable that a lawsuit and liability could ensue. It may also have unintended insurance consequences—specifically that insurance coverage could be voided or otherwise denied on grounds that the company "should have known" of threats to covered assets but failed to disclose them to

insurers and failed to take the necessary precautions recommended by the information-sharing group.

Liability in both situations may be minimized by explicitly excluding from the membership agreement the duty to disclose or use information gained through participation in an information-sharing group. Such an agreement will establish clearly the duties of each member related to the accurate reporting of information (which may be that there is no duty) and the handling of reported information (which could, for example, mandate the use of certain technological measures for data-handling). It will also establish penalties for the failure to carry out one's duty. Any company that chooses to sign such a contract should thus be aware of the legal obligations that it generates.

Legal Issues Related to Industry Sharing Information with the Government

Systems of cooperation and coordination aimed at protecting the nation's critical infrastructures can be enhanced by the participation of the government, both at federal and state levels. The government has access to data and intelligence that is unavailable in the private sector and could be quite valuable in defending against a cyber attack. Government involvement, however, where both sides give and acquire information raises concerns of privacy, liability, and security amongst potential industry participants. These concerns and the existing legal regime must be considered and weighed against the ultimate objectives of any public-private partnership to secure and strengthen the nation's critical infrastructures.

- **The Freedom of Information Act (5 U.S.C. § 522).** The Freedom of Information Act (FOIA) permits "any person" to seek access to any government "agency record" that is not subject to one of nine exemptions or three special law enforcement exclusions. If voluntary disclosure is desired by the government in a future infrastructure protection initiative, close attention should be given to whether these exemptions would sufficiently protect from public disclosure the sensitive business information that might have to be disclosed to a governmental agency.

  Exemption 4 of FOIA provides protection for certain business information shared with the federal government. This exemption protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C. §552(b)(4)). The exemption is meant to encourage persons to voluntarily furnish useful commercial or financial information to the government by safeguarding it from the competitive disadvantage that could result from disclosure. The two-way sharing of information under this exemption has not yet been tested by the other ISACs, but it could be a viable solution until a formal legislative amendment to FOIA passes the Congress.

  One strategy that may be effective in reducing or eliminating concerns about the release of sensitive information under FOIA is to enter into a Memorandum of Understanding (MOU) or other similar agreement with the federal agency with whom the information sharing is taking place. The agreement could specify whether information is being submitted under any FOIA exemption and could also govern how the information will be handled and to whom it would be disclosed. MOUs and their applicability are discussed further below.

- **The Privacy Act (5 U.S.C. § 552a).** The Privacy Act provides that any personal information concerning U.S. citizens and permanent-resident aliens that is maintained in a "system of records" may not be disclosed unless that disclosure is permitted under one of several specific exceptions. One such exemption allows the head of any agency to exempt a "system of records" from disclosure if the principal

function of the system includes the enforcement of criminal laws and the records consist of information compiled for the purpose of a criminal investigation.

The crucial legal concern with respect to FOIA and the Privacy Act is whether these exemptions are broad enough to ensure that sensitive business information and informant identities remain confidential vis-a-vis the public and competitors while, at the same time, limited enough to ensure that the appropriate agency or agencies can access information needed to deal with threats to critical infrastructure security.

- **Protection of Trade Secrets.** A related concern is the potential loss of protection for trade secrets (or other proprietary information). Trade secret protections are an advantage to many companies because they provide for the possibility of perpetual protection, they can be maintained without the cost involved in patenting (nor do they require the disclosure of invention details to the public). Moreover, a trade secret need not be a significant or important advance but, rather, can be any information, design, device, process, composition, technique, or formula that is not known generally and that affords its owner a competitive business advantage. Because a fundamental requirement associated with trade protection is that the thing protected not be known generally, the risk that voluntary disclosure of trade secret information to the government may intentionally be given to or inadvertently end up in the hands of the general public and, consequently, that trade secret protection will be lost, is a major disincentive to voluntary disclosure of this type of information by the private sector.

- **Sunshine Laws.** Any effort to promote information sharing by state or local governments must take account of the general inconsistency among state "Sunshine Laws" requiring the public disclosure of certain proceedings by public bodies. While states commonly exempt meetings concerning matters of public security from their Sunshine Laws, there is considerable disparity among states' Sunshine Laws and their application by the courts. In the area of law enforcement, states' efforts to strike a balance between personal privacy and public access to information have resulted in varying sunshine law exemptions that provide only general guidance for authorities and requesters of information. In addition, some states have modeled their exemptions after the federal FOIA, to varying degrees, while others have relied on their own legislators' lawmaking ability.

The issues raised above force any industry considering the establishment of an information-sharing program to think seriously about the advantages and disadvantages of giving the government a role in that program. There is no right answer in this case, as the decision depends solely on the industry's willingness to accept certain tradeoffs, in return for the advantage of having the government's assistance and input. It seems that for nearly each partnership that remains privately based, there is a similar public-private arrangement that functions just as well. The distinguishing feature of these latter arrangements is that they are based on clear agreements as to the role and function of each player involved. The most significant of those agreements is an MOU with the participating government agency or agencies as to the appropriate use and/or disclosure of the information obtained through participation. As with the membership agreement, it can also absolve private-sector participants from the duty to report information on attacks to the government. An MOU will not be easy to negotiate, but could be key to any arrangement that envisions a public-private partnership for critical infrastructure protection.

Independent Disclosure of Information to the Government

If industry and government cannot come to acceptable terms for information sharing, a

company may still choose to report independently to the government on some critical infrastructure vulnerabilities. In contrast to the impediments to disclosure discussed above, one such way to ensure the smooth and trusted exchange of information with the government is through a confidentiality statement or nondisclosure agreement. These agreements are already being used widely in the private sector and by governmental agencies. For example, the U.S. Department of Energy (DOE) has created a Sample Nondisclosure and Confidentiality Agreement. It is intended to serve as a template for addressing terms and conditions that might be involved in establishing a multi-party non-disclosure and confidentiality agreement pursuant to efforts of the DOE's Infrastructure Assurance Outreach Program and to prevent inappropriate disclosure of proprietary or sensitive business information. It is possible that the use of similar agreements may be an important part of information sharing as part of infrastructure assurance.

The use of confidentiality/non-disclosure guarantees in the context of infrastructure assurance would create a number of potential complications that would have to be resolved before industry participants would be comfortable relying upon them. This includes whether information disclosed to the government could be further disclosed, and whether the disclosing company would be liable for any further disclosures, either intentional or inadvertent.

These issues would need to be addressed prior to the implementation of a model for infrastructure assurance that incorporates the use of such agreements.

EXAMPLES OF INFORMATION SHARING PARTNERSHIPS

The discussion above is not meant to generate doubts as to the feasibility of information-sharing arrangements, for such arrangements do exist and have been quite successful. The following are examples of both public and public-private information sharing partnerships. It is hoped that these examples will be helpful as the energy industry works with the government and with companies within its own industry to design a system for critical infrastructure assurance.

Private-Sector Models

Industry participants have already demonstrated that they can work together to share information in appropriate areas. Two examples are especially illustrative.

- **Financial Services Information Sharing and Analysis Center (FS/ISAC).** The financial services sector established an ISAC in October 1999 as a limited liability corporation. FS/ISAC members have access to information and analysis relating to information provided by other members, the federal government, law enforcement agencies, and information security associations. Membership is open to U.S. chartered companies in the banking, securities, and insurance industries; however, the federal government is not allowed to access the FS/ISAC database. The FS/ISAC gained recognition when it successfully distributed warnings about the February 2000 denial of service attacks and the Love Bug virus.

- **Information Technology Information Sharing and Analysis Center (IT/ISAC).** The ISAC for the information technology sector was publicly proposed in January 2001. The IT/ISAC is a not-for-profit corporation and facilitates the reporting and exchange of information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. Although the IT/ISAC is currently only composed of its 19 founding technology company members, membership is open, and many major U.S. based technology and telecommunications firms are expected to join. While the federal government was instrumental in assisting in the formation of the

IT/ISAC, it will not play an immediate role in the organization.

Public-Private Sector Models

The following collaborative efforts between public- and private-sector entities can serve as models for similar efforts between the petroleum industry and government with respect to the security of the industry's critical infrastructure.

- **Sharing of Information Consistent with the Nuclear Regulatory Commission Regulations.** The Nuclear Regulatory Commission permits nuclear power plants to share information with the Commission and with each other about potential safety risks, including possibly dangerous employees. Importantly, the companies that share information are protected from possible liabilities arising out of this information sharing (e.g., the risk of a defamation claim by a former employee).

- **International Energy Agency.** The International Energy Agency is an organization of 25 member countries created to address oil supply emergencies. The members share energy information and coordinate their energy policies. U.S. petroleum companies participate in information exchanges under a specific exemption from the U.S. antitrust laws. Periodically, Congress reconsiders this exemption.

- **National Security Telecommunications Advisory Committee and National Communications System.** This is a collaboration between the private National Security Telecommunications Advisory Committee (comprised of the leading U.S. telecommunications companies) and the government's National Communications System (a confederation of 23 federal government entities). The two groups, charged jointly with ensuring the robustness of the national telecommunications grid, have been working together since 1984 and share information about threats, vulnerabilities, operations, and incidents, which improves the overall security of the telecommunications infrastructure.

- **Centers for Disease Control.** The federal Centers for Disease Control (CDC) has developed, over time, a system for acquiring medical data relating to areas of public interest for purposes of analysis. Toward this end, the CDC cooperates with state agencies and other responsible individuals, obtaining information as anonymous data in an effort to protect the privacy of individual patients. The CDC's efforts to eliminate identifiable personal information from its databases are crucial to facilitating information exchange and promoting trust in the system. The petroleum industry should require similar assurances if it is to be asked or required to provide proprietary information to the government in an effort to combat terrorist threats to the industry.

LEGISLATIVE INITIATIVES TO ENCOURAGE INFORMATION SHARING

Several bills introduced in the last session of Congress would have helped to remove or reduce some of industry's concerns about sharing critical infrastructure information with the government, notably by creating a new exemption from the Freedom of Information Act for information shared for network defense purposes. One such bill was the proposed Cyber Security Information Act (H.R. 4246, 106th Congress, April 12, 2000). This proposed legislation encouraged secure disclosure and protected information exchanges in connection with infrastructure assurance. The bill was designed to exempt cyber security data from the Freedom of Information Act, prevent its disclosure to third parties, and exempt its use "by any Federal or State entity, agency, or authority or by any third party, directly or indirectly, in any civil action arising under any Federal or State law." The bill also contained an antitrust exemption for exchanges of information to facilitate or "to help correct or avoid the effects of a

cyber security problem." However, the bill contained an exception to the above-noted exemption when applied to conduct that involves or results "in an agreement to boycott any person, to allocate a market, or to fix prices or output." Whether this exception to the exemption would chill certain legitimate disclosures is an issue that was not considered. The bill would have permitted the President to establish working groups of federal employees to engage outside organizations to share information and facilitate the purposes of the proposed legislation.

If the proposed Cyber Security Information Act had been enacted, it would have served as a model to shield other beneficial exchanges of information that supports infrastructure assurance from potential legal consequences. Similar legislation is expected to be reintroduced in the 107th Congress. These initiatives should be closely monitored by industry participants seeking to establish public-private partnerships for critical infrastructure protection.

FINDINGS AND CONCLUSIONS

- Obtaining a business review letter from the Department of Justice can minimize the risk of antitrust liability for information sharing.
- An ISAC should be structured to ensure that there is no violation of privacy rights.
- Companies should have a good faith basis to disseminate unfavorable information when necessary about a particular product or person that poses a threat to the security of the industry's critical infrastructures.
- In the formation and operation of an ISAC, most of the potential liability can be minimized through an effective allocation of the risks through several contractual arrangements, such as the ISAC membership agreement, service agreement with ISAC provider, and ISAC membership rules.
- Sharing information with the government may lead to unwanted disclosure of the information to third parties pursuant to the Freedom of Information Act. However, with a properly structured formal memorandum of understanding or other similar agreement it is possible to share information with the government.
- Other information-sharing mechanisms, such as the FS/ISAC, are in operation, and are successfully dealing with the legal and liability issues.

CHAPTER 7

Research and Development Needs

The research and development (R&D) goal in support of critical infrastructure protection should be the development of technologies and processes that will reduce vulnerabilities and counter threats in those areas having the potential for causing significant national security, economic, and/or social impacts. The oil and natural gas industries primarily rely on commercial providers for R&D in information technology, telecommunications, and supervisory control and data acquisition (SCADA) systems. Consequently, the oil and natural gas industries have few core competencies in these areas.

Government-funded R&D should address national security and key critical infrastructure protection issues that transcend the capabilities of individual companies in the oil and natural gas sector. The government should work with industry to focus and prioritize their R&D program and ensure that mechanisms exist to rapidly transfer the results that enhance critical infrastructure protection.

In 1996, the President's Commission on Critical Infrastructure Protection identified several common R&D themes that crosscut all critical infrastructures:

- Protecting infrastructures
- Detecting intrusions
- Mitigating the effects of disruptions
- Facilitating recovery
- Developing analytical or supporting technologies.

The challenge for government is to work with the oil and natural gas industries and the other critical infrastructures to help focus R&D, leverage existing technologies, and enhance critical infrastructure protection. An important ingredient in this cooperative effort will be the technology transfer to industry from government of the pertinent results from the R&D work.

PROPOSED RESEARCH AND DEVELOPMENT NEEDS

The R&D needs proposed in this section are from the perspective of the oil and natural gas industries. They range from specific information technology, telecommunications, and interdependencies to issues related to physical asset protection. The majority of the needs would be of value to other infrastructures as well.

- **Information Assurance.** As national infrastructures increasingly depend on computers and networked information systems to improve efficiency and enhance economic competitiveness, they also become more vulnerable to potential cyber attacks. In addition, the basic technology is changing rapidly, open architectures are being pursued, and globalization is intensifying competition. These changes affect both the individual critical infrastructures and the national interdependent infrastructures. Significant new investments in R&D are required to protect the information technology and telecommunications infrastructures, and the information created, stored, processed, and transmitted on it.

- **Interdependencies and Systems Complexity.** The energy infrastructures depend strongly on computers and computing systems for operations and communication along with all other critical infrastructures. The energy infrastructures

also depend on itself (e.g., dependencies between oil and natural gas and electric power). Advanced methods and tools for vulnerability assessment and systems analysis are needed to identify critical nodes within infrastructures, examine interdependencies, and help understand the behavior of these complex systems. Modeling and simulation tools and test beds for studying infrastructure-related problems are essential for understanding the interdependent infrastructures.

- **Physical Protection Assessment.** Research will result in enhancements focused on the protection of physical assets of the oil and natural gas industries, current protection methods, and strategies for future protection.

- **Multisensor and Warning Technologies.** Central to the protection of any infrastructure is the implementation of an integrated, collaborative system of overlapping cyber technologies designed to warn against intruders at any of the critical facilities and control nodes along that system. The proposed integrated Multi-sensor and Warning Technologies (MSWT) system would further facilitate analysis of data to provide information that can be used to anticipate attacks and identify perpetrators.

- **Protection and Mitigation.** Real-time system control, infrastructure hardening, and containment technologies are needed to protect infrastructure systems against threats and mitigate the impacts of disruptions. Advanced survivability, reliability, and assurance enhancement measures need to be explored and developed. Technologies are needed to contain and isolate the impacts of information system disruption so that the complete system or dependent infrastructures are not affected.

- **Risk Management.** Improved methodologies and tools are needed to identify and manage risks to infrastructures and information. Research areas include developing methodologies for measuring the relative risks and the degree of impact of infrastructure assurance investment strategies; for enhancing the ability of users to perform consequence assessment and risk analysis; for developing effective risk management approaches and strategies; for dealing with uncertainties in, or incomplete knowledge of, threats, vulnerabilities, and protection measures; and for managing risks across the multiple components and organizations involved in the infrastructures. Methods also are needed to more effectively characterize risks and communicate risk information.

- **Critical Consequence Analysis.** This R&D topic would develop a thorough understanding of the possible consequences of physical and cyber failures, as well as strategies for coping with them.

- **SCADA Protection Enhancement.** The oil and natural gas industries' SCADA systems are increasingly being linked with electronic business systems and are therefore becoming more vulnerable to cyber intrusion. This task will assist in developing a viable method to economically enhance the security of SCADA systems.

- **Monitoring and Detection.** A protection and attack sensing and warning capability is needed to provide early threat warning to government organizations and private-sector infrastructure owners and operators, thereby preventing widespread infrastructure disruptions that have potentially serious consequences on our national security, economy, and quality of life.

- **Modeling and Simulation.** Modeling and simulation tools and environments (e.g., test beds) need to be developed for studying infrastructure-related problems and dynamic response mechanisms under varying conditions. Such tools allow experimentation that cannot be performed in realistic environments of any appreciable scale. For example, robust infrastructure and nodal analysis techniques and tools need to be

developed for modeling large-scale distributed/networked systems and interdependent infrastructures. Such tools would support systems analysis and decision making.

- **Decision Support.** Decision support methodologies, tools, and information systems are needed to help identify and prioritize critical assets for protection, mitigation, incident management, and recovery; compute return on investment in completing security technologies; and develop overall infrastructure assurance investment strategies. Measurable criteria also need to be established that address national security, economic competitiveness, quality of life, and other important attributes. Such methodologies, tools, and information systems would help determine what infrastructure assets are critical, and thus aid in the priority use of resources in a degraded environment.

- **Institutional Barriers.** This research topic focuses on institutional issues that are potential impediments to the successful implementation of critical infrastructure protection. Accordingly, it is based more on the disciplines of policy and operations research than on technological disciplines. The result of this research and analysis is a series of plans that recognize and address the potential strategic, policy, and structural constraints facing an initiative that embraces national coordination and alignment to a common set of priorities. The plans may include operating charters in which teams are either involved or proposed

FINDINGS AND CONCLUSIONS

- The oil and natural gas industries primarily rely on commercial providers for R&D in the areas of information technology, telecommunication, electronic commerce, and SCADA systems and related critical infrastructure protection security.

- Government-funded research is appropriate where the issues transcend individual industries and address national security needs. Availability of the results of such research will aid industry's efforts in protecting their critical infrastructures. This effort will require cooperation among infrastructure owners and operators along with government and their research organizations.

- The unique challenge for government will be the concomitant technology transfer plan that will accelerate the introduction of infrastructure assurance measures to the oil and natural gas industries and other key infrastructures in the private sector.

APPENDICES

Appendix A
Request Letters
and Description of the
National Petroleum Council

Appendix B
Study Group Rosters

The Secretary of Energy
Washington, DC 20585

April 7, 1999

Mr. Joe B. Foster
Chair
National Petroleum Council
1625 K Street, N.W.
Washington, D.C. 20006

Dear Mr. Foster:

Thank you for your letter of December 14, 1998. I am writing to formally request the Council's advice on cooperative approaches to protecting the critical infrastructure of the United States oil and gas industry.

The Federal Government is aggressively pursuing a variety of approaches through which the critical infrastructures of the United States can be protected from physical and cyber threats. To be effective, however, these approaches must be developed and implemented in partnership with the industry because the private sector owns and controls the vast majority of the Nation's critical infrastructures. You have indicated that the Council believes it can contribute meaningfully to these efforts and can provide advice on a systematic approach to the planning process for protecting the critical infrastructures of the oil and gas industry.

Accordingly, I request the National Petroleum Council to review the potential vulnerabilities of the oil and gas industries to attack--both physical and cyber--and to advise me on policies and practices that industry and Government, separately and in partnership, should adopt to protect or recover from such attacks.

Specifically, I would like the Council to advise me on:

1. definitions of criticality and risk in the context of critical infrastructure protection of oil and gas system infrastructures;

2. remedies for legal concerns such as protection of confidential information and the ability of competing firms to participate in cooperative relationships, and

3. mechanisms through which the industry can beneficially access relevant Federal law enforcement and intelligence assets and through which industry can both benefit from and help prioritize Government research and development programs in infrastructure assurance.

Finally, Presidential Decision Directive 63, which implements the recommendation of the President's Commission on Critical Infrastructure Protection, calls for me to designate a Sector Coordinator for the oil and gas industry. For the duration of your study, I would like the National Petroleum Council to take on the responsibility of the Sector Coordinator. At the conclusion of your work, I would like your advice on the permanent role of the Sector Coordinator and your recommendation on how that person or organization should be identified. The North American Electric Reliability Council has been designated as the Sector Coordinator for the electric industry and, in recognition of the growing interrelationship between the gas and electric industries, you should collaborate with that group as appropriate. Further, the Departments of Transportation and Energy have agreed to share critical infrastructure protection responsibilities for the Nation's oil and gas pipeline systems. Your advice, therefore, should consider oil and gas infrastructures from production to consumption.

Given the nature of this request, Under Secretary Ernest J. Moniz will represent the Department and will provide appropriate coordination with the Department of Transportation and other branches of Government.

As always, I appreciate the Council's ongoing assistance in these issues of national policy and mutual concern.

Yours sincerely,

Bill Richardson

cc: Richard Clarke
Rodney E. Slater
Erle Nye
Michehl Gent

The Secretary of Energy
Washington, DC 20585

October 15, 1999

Mr. Joe B. Foster
Chair
National Petroleum Council
1625 K Street, N.W.
Washington, D.C. 20006-1656

Dear Mr. Foster:

This letter conveys my approval to establish a Committee on Critical Infrastructure Protection and to appoint the members of the Committee as proposed in your letter of August 9, 1999.

The Government Co-chair for the Committee will be retired Air Force General Eugene E. Habiger, Director of the recently established Office of Security and Emergency Operations. The Office of Fossil Energy has substantial interest in this topic and will continue to work cooperatively with the Office of Security and Emergency Operations to address critical infrastructure issues related to the electricity, oil and gas industries.

I am pleased that the National Petroleum Council has accepted responsibility for reviewing the potential vulnerabilities of our Nation's oil and gas critical infrastructure and advising me on policies and practices that Government and industry, separately and in partnership, should adopt to ensure its integrity. The Council's willingness to additionally serve as the interim Sector Coordinator for the oil and gas industry for the duration of your study is deeply appreciated.

Yours sincerely,

Bill Richardson

Bill Richardson

Description of the National Petroleum Council

In May 1946, the President stated in a letter to the Secretary of the Interior that he had been impressed by the contribution made through government/industry cooperation to the success of the World War II petroleum program. He felt that it would be beneficial if this close relationship were to be continued and suggested that the Secretary of the Interior establish an industry organization to advise the Secretary on oil and natural gas matters.

Pursuant to this request, Interior Secretary J. A. Krug established the National Petroleum Council (NPC) on June 18, 1946. In October 1977, the Department of Energy was established and the Council was transferred to the new department.

The purpose of the NPC is solely to advise, inform, and make recommendations to the Secretary of Energy on any matter, requested by the Secretary, relating to oil and natural gas or the oil and gas industries. Matters that the Secretary of Energy would like to have considered by the Council are submitted in the form of a letter outlining the nature and scope of the study. The Council reserves the right to decide whether it will consider any matter referred to it.

Examples of studies undertaken by the NPC at the request of the Secretary of Energy include:

- *Factors Affecting U.S. Oil & Gas Outlook (1987)*
- *Integrating R&D Efforts (1988)*
- *Petroleum Storage & Transportation (1989)*
- *Industry Assistance to Government – Methods for Providing Petroleum Industry Expertise During Emergencies (1991)*
- *Short-Term Petroleum Outlook – An Examination of Issues and Projections (1991)*
- *Petroleum Refining in the 1990s – Meeting the Challenges of the Clean Air Act (1991)*
- *The Potential for Natural Gas in the United States (1992)*
- *U.S. Petroleum Refining – Meeting Requirements for Cleaner Fuels and Refineries (1993)*
- *The Oil Pollution Act of 1990: Issues and Solutions (1994)*
- *Marginal Wells (1994)*
- *Research, Development, and Demonstration Needs of the Oil and Gas Industry (1995)*
- *Future Issues – A View of U.S. Oil & Natural Gas to 2020 (1995)*
- *Issues for Interagency Consideration – A Supplement to the NPC's Report: Future Issues – A View of U.S. Oil & Natural Gas to 2020 (1996)*
- *U.S. Petroleum Product Supply – Inventory Dynamics (1998)*
- *Meeting the Challenges of the Nation's Growing Natural Gas Demand (1999)*
- *U.S. Petroleum Refining – Assuring the Adequacy and Affordability of Cleaner Fuels (2000).*

The NPC does not concern itself with trade practices, nor does it engage in any of the usual trade association activities. The Council is subject to the provisions of the Federal Advisory Committee Act of 1972.

Members of the National Petroleum Council are appointed by the Secretary of Energy and represent all segments of the oil and gas industries and related interests. The NPC is headed by a Chair and a Vice Chair, who are elected by the Council. The Council is supported entirely by voluntary contributions from its members.

NATIONAL PETROLEUM COUNCIL

MEMBERSHIP

2000/2001

Jacob Adams
President
Arctic Slope Regional Corporation

Robert O. Agbede
President and
Chief Executive Officer
Advanced Technology Systems, Inc.

George A. Alcorn
President
Alcorn Exploration, Inc.

Benjamin B. Alexander
President
Dasco Energy Corporation

Conrad K. Allen
Vice President
National Association of Black Geologists
and Geophysicists

Robert J. Allison, Jr.
Chairman and
Chief Executive Officer
Anadarko Petroleum Corporation

Robert O. Anderson
Roswell, New Mexico

Philip F. Anschutz
President
The Anschutz Corporation

Gregory L. Armstrong
Chairman and
Chief Executive Officer
Plains All American

Robert G. Armstrong
President
Armstrong Energy Corporation

O. Truman Arnold
Chairman of the Board and
Chief Executive Officer
Truman Arnold Companies

Ralph E. Bailey
Chairman and
Chief Executive Officer
Xpronet Inc.

D. Euan Baird
Chairman, President and
Chief Executive Officer
Schlumberger Limited

William W. Ballard
President
Ballard Petroleum, L.L.C.

William J. Barrett
Chairman and
Chief Executive Officer
Barrett Resources Corporation

Gonzalo Barrientos
State Senator
The Senate of
The State of Texas

Michael L. Beatty
Michael L. Beatty & Associates

Riley P. Bechtel
Chairman and
Chief Executive Officer
Bechtel Group, Inc.

David W. Biegler
President and
Chief Operating Officer
TXU

Peter I. Bijur
Retired Chairman of the Board
Texaco Inc.

M. Frank Bishop
Executive Director
National Association of
State Energy Officials

Carl E. Bolch, Jr.
Chairman and
Chief Executive Officer
Racetrac Petroleum, Inc.

John F. Bookout
Houston, Texas

Charles T. Bryan
President and
Chief Executive Officer
DeGolyer and MacNaughton Inc.

Carl Burhanan
President
Oasis Aviation, Inc.

Victor A. Burk
Managing Partner
Global Energy & Utilities
Arthur Andersen, L.L.P.

Frank M. Burke, Jr.
Chairman and
Chief Executive Officer
Burke, Mayborn Company, Ltd.

Charles William Burton
Partner
Jones, Day, Reavis & Pogue

Karl R. Butler
President and
Chief Executive Officer
ICC Energy Corporation

George Campbell, Jr.
President
The Cooper Union for the
Advancement of Science and Art

Philip J. Carroll
Chairman and
Chief Executive Officer
Fluor Corporation

R. D. Cash
Chairman and
Chief Executive Officer
Questar Corporation

Robert B. Catell
Chairman and
Chief Executive Officer
KeySpan

Clarence P. Cazalot, Jr.
President
Marathon Oil Company

Paul W. Chellgren
Chairman of the Board and
Chief Exceutive Officer
Ashland Inc.

Danny H. Conklin
Partner
Philcon Development Co.

Luke R. Corbett
Chairman and
Chief Executive Officer
Kerr-McGee Corporation

Michael B. Coulson
President
Coulson Oil Co.

Gregory L. Craig
President
Cook Inlet Energy Supply

Hector J. Cuellar
Managing Director
Area/Industries Manager
Bank of America

William A. Custard
President and
Chief Executive Officer
Dallas Production, Inc.

Robert Darbelnet
President and
Chief Executive Officer
AAA

George A. Davidson, Jr.
Retired Chairman
Dominion Resources, Inc.

Claiborne P. Deming
President and
Chief Executive Officer
Murphy Oil Corporation

Cortlandt S. Dietler
President and
Chief Executive Officer
TransMontaigne Oil Company

David F. Dorn
Chairman Emeritus
Forest Oil Corporation

John G. Drosdick
Chairman, President and
Chief Executive Officer
Sunoco, Inc.

Archie W. Dunham
Chairman, President and
Chief Executive Officer
Conoco Inc.

W. Byron Dunn
President and
Chief Executive Officer
Lone Star Steel Company

Daniel C. Eckermann
President and
Chief Executive Officer
LeTourneau, Inc.

James W. Emison
Chairman and
Chief Executive Officer
Western Petroleum Company

Ronald A. Erickson
Chief Executive Officer
Holiday Companies

Sheldon R. Erikson
Chairman of the Board, President
and Chief Executive Officer
Cooper Cameron Corporation

John G. Farbes
President
Big Lake Corporation

Thomas L. Fisher
Chairman, President and
Chief Executive Officer
Nicor Inc.

William L. Fisher
Leonidas T. Barrow Chair in
Mineral Resources
Department of Geological Sciences
University of Texas at Austin

James C. Flores
Chairman, President and
Chief Executive Officer
Sable Minerals, Inc.

Douglas L. Foshee
Houston, Texas

Joe B. Foster
Non-executive Chairman
Newfield Exploration Company

Robert W. Fri
Director
The National Museum of
Natural History
Smithsonian Institution

J. E. Gallegos
Attorney
Energy & Environmental Law
Gallegos Law Firm

Jean Gaulin
Chairman, President and
Chief Executive Officer
Ultramar Diamond Shamrock Corp.

Murry S. Gerber
President and
Chief Executive Officer
Equitable Resources

James A. Gibbs
President
Five States Energy Company

Rufus D. Gladney
Chairman
American Association of Blacks in Energy

Alfred R. Glancy III
Retired Chairman of the Board
MCN Energy Group Inc.

Bruce C. Gottwald
Chairman of the Board
Ethyl Corporation

S. Diane Graham
Chairman and
Chief Executive Officer
STRATCO, Inc.

Frederic C. Hamilton
Chairman
The Hamilton Companies

Christine Hansen
Executive Director
Interstate Oil and Gas
Compact Commission

Michael F. Harness
President
Osyka Corporation

Angela E. Harrison
Chairman and
Chief Executive Officer
WELSCO, Inc.

Timothy C. Headington
President/Owner
Headington Oil Company

John B. Hess
Chairman of the Board and
Chief Executive Officer
Amerada Hess Corporation

Jack D. Hightower
Chairman of the Board, President
and Chief Executive Officer
Pure Resources, Inc.

Jerry V. Hoffman
Chairman, President and
Chief Executive Officer
Berry Petroleum Company

R. Earl Holding
President and
Chief Executive Officer
Sinclair Oil Corporation

Roy M. Huffington
Chairman of the Board and
Chief Executive Officer
Roy M. Huffington, Inc.

Ray L. Hunt
Chairman of the Board
Hunt Oil Company

James M. Hutchison
President
HUTCO Inc.

Frank J. Iarossi
Chairman and
Chief Executive Officer
American Bureau of Shipping &
Affiliated Companies

Eugene M. Isenberg
Chairman and
Chief Executive Officer
Nabors Industries, Inc.

A. V. Jones, Jr.
Chairman
Van Operating, Ltd.

Jon Rex Jones
Chairman
EnerVest Management Company, L. C.

Jerry D. Jordan
President
Jordan Energy Inc.

Fred C. Julander
President
Julander Energy Company

Robert Kelley
Retired Chairman of the Board
Noble Affiliates, Incorporated

Bernard J. Kennedy
Chairman and
Chief Executive Officer
National Fuel Gas Company

Richard D. Kinder
Chairman and
Chief Executive Officer
Kinder Morgan Energy Partners, L.P.

Harold M. Korell
President and
Chief Executive Officer
Southwestern Energy Company

Fred Krupp
Executive Director
Environmental Defense Fund

Susan M. Landon
Petroleum Geologist

Kenneth L. Lay
Chairman of the Board
Enron Corp.

Stephen D. Layton
President
E&B Natural Resources

Virginia B. Lazenby
Chairman and
Chief Executive Officer
Bretagne G.P.

Lila Leathers
President and
Chief Executive Officer
Leathers Oil Co.

David L. Lemmon
President and
Chief Executive Officer
Colonial Pipeline Company

David J. Lesar
Chairman of the Board, President
and Chief Executive Officer
Halliburton Company

John H. Lichtblau
Chairman and
Chief Executive Officer
Petroleum Industry Research
Foundation, Inc.

Daniel H. Lopez
President
New Mexico Institute of
Mining and Technology

Thomas E. Love
Chairman and
Chief Executive Officer
Love's Country Stores, Inc.

William D. McCabe
Director of Energy Resources & Supply
Council of Energy Resource Tribes

Ferrell P. McClean
Managing Director
J. P. Morgan Securities Inc.

S. Todd Maclin
Managing Director and
Global Oil & Gas Group Executive
J. P. Morgan Securities Inc.

Cary M. Maguire
President
Maguire Oil Company

Robert A. Malone
Regional President for the
Western United States
BP p.l.c.

Timothy M. Marquez
President and
Chief Executive Officer
Venoco, Inc.

Frederick R. Mayer
Chairman
Captiva Resources, Inc.

F. H. Merelli
Chairman and
Chief Executive Officer
Key Production Company, Inc.

C. John Miller
Chief Executive Officer
Miller Energy, Inc.

Steven L. Miller
Chairman, President and
Chief Executive Officer
Shell Oil Company

Claudie D. Minor, Jr.
President and
Chief Executive Officer
Premier Energy Supply Corp.

George P. Mitchell
Chairman of the Board and
Chief Executive Officer
Mitchell Energy and Development Corp.

Mark E. Monroe
President and
Chief Executive Officer
Louis Dreyfus Natural Gas

Herman Morris, Jr.
President and
Chief Executive Officer
Memphis Light, Gas & Water Division

James J. Mulva
Chairman of the Board and
Chief Executive Officer
Phillips Petroleum Company

John Thomas Munro
President
Munro Petroleum &
Terminal Corporation

Mark B. Murphy
President
Strata Production Company

Gary L. Neale
Chairman, President and
Chief Executive Officer
NiSource Inc.

J. Larry Nichols
Chairman of the Board, President
and Chief Executive Officer
Devon Energy Corporation

René O. Oliveira
State Representative
The House of Representatives of
The State of Texas

David J. O'Reilly
Chairman of the Board and
Chief Executive Officer
Chevron Corporation

C. R. Palmer
Chairman of the Board, President
and Chief Executive Officer
Rowan Companies, Inc.

Mark G. Papa
Chairman and
Chief Executive Officer
EOG Resources, Inc.

Paul H. Parker
Vice President
Center for Resource Management

Robert L. Parker, Sr.
Chairman of the Board
Parker Drilling Company

Emil Peña
President and
Chief Executive Officer
Generation Power Inc.

L. Frank Pitts
Owner
Pitts Energy Group

Richard B. Priory
Chairman and
Chief Executive Officer
Duke Energy Corporation

Caroline Quinn
President
Farrar Oil Company

Daniel Rappaport
Former Chairman of the Board
New York Mercantile Exchange

Edward B. Rasmuson
Chairman of the Board and
Chief Executive Officer
National Bank of Alaska

Lee R. Raymond
Chairman, President and
Chief Executive Officer
Exxon Mobil Corporation

John G. Rice
President and
Chief Executive Officer
GE Power Systems

Corbin J. Robertson, Jr.
President
Quintana Minerals Corporation

Robert E. Rose
Chairman, President and
Chief Executive Officer
Global Marine Inc.

Henry A. Rosenberg, Jr.
Chairman of the Board
Crown Central Petroleum Corporation

A. R. Sanchez, Jr.
Chairman of the Board and
Chief Executive Officer
Sanchez-O'Brien Oil and Gas Corporation

Robert Santistevan
Director
Southern Ute Indian Tribe
Growth Fund

S. Scott Sewell
President
Delta Energy Management, Inc.

Bobby S. Shackouls
Chairman, President and
Chief Executive Officer
Burlington Resources Inc.

Donald M. Simmons
Muskogee, Oklahoma

Matthew R. Simmons
President
Simmons and Company International

Arlie M. Skov
President
Arlie M. Skov, Inc.

Arthur L. Smith
Chairman
John S. Herold, Inc.

Bruce A. Smith
Chairman, President and
Chief Executive Officer
Tesoro Petroleum Corporation

Joel V. Staff
Chairman and
Chief Executive Officer
National-Oilwell, Inc.

Charles C. Stephenson, Jr.
Chairman of the Board
Vintage Petroleum, Inc.

James H. Stone
Chairman of the Board
Stone Energy Corporation

Carroll W. Suggs
Chairman of the Board, President
and Chief Executive Officer
Petroleum Helicopters, Inc.

Patrick F. Taylor
Chairman and
Chief Executive Officer
Taylor Energy Company

Richard E. Terry
Chairman and
Chief Executive Officer
Peoples Energy Corporation

Gerald Torres
Associate Dean for Academic Affairs
University of Texas School of Law and
Vice Provost
University of Texas at Austin

H. A. True, III
Partner
True Oil Company

Randy E. Velarde
President
The Plaza Group

Thurman Velarde
Administrator
Oil and Gas Administration
Jicarilla Apache Tribe

Philip K. Verleger, Jr.
PKVerleger, L.L.C.

Joseph C. Walter, III
President
Walter Oil & Gas Corporation

L. O. Ward
Owner-President
Ward Petroleum Corporation

C. L. Watson
Chairman of the Board and
Chief Executive Officer
Dynegy Inc.

Michael E. Wiley
Chairman, President and
Chief Executive Officer
Baker Hughes Incorporated

Bruce W. Wilkinson
Chairman of the Board and
Chief Executive Officer
McDermott International, Inc.

Mary Jane Wilson
President and
Chief Executive Officer
WZI Inc.

Irene S. Wischer
President and
Chief Executive Officer
Panhandle Producing Company

Brion G. Wise
Chairman and
Chief Executive Officer
Western Gas Resources, Inc.

William A. Wise
Chairman, President and
Chief Executive Officer
El Paso Corporation

George M. Yates
President and
Chief Executive Officer
Harvey E. Yates Company

John A. Yates
President
Yates Petroleum Corporation

Daniel H. Yergin
President
Cambridge Energy Research Associates

Henry Zarrow
Vice Chairman
Sooner Pipe & Supply Corporation

COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

CHAIR

David J. Lesar
Chairman of the Board, President
and Chief Executive Officer
Halliburton Company

ACTING GOVERNMENT COCHAIR*

Paula L. Scalingi
Director
Office of Critical Infrastructure Protection
U.S. Department of Energy

EX OFFICIO

Archie W. Dunham
Chair
National Petroleum Council

EX OFFICIO

William A. Wise
Vice Chair
National Petroleum Council

SECRETARY

Marshall W. Nichols
Executive Director
National Petroleum Council

* * *

Riley P. Bechtel
Chairman and
Chief Executive Officer
Bechtel Group, Inc.

David W. Biegler
President and
Chief Operating Officer
TXU

Peter I. Bijur
Retired Chairman of the Board
Texaco Inc.

M. Frank Bishop
Executive Director
National Association of
State Energy Officials

Philip J. Carroll
Chairman and
Chief Executive Officer
Fluor Corporation

R. D. Cash
Chairman and
Chief Executive Officer
Questar Corporation

Robert B. Catell
Chairman and
Chief Executive Officer
KeySpan

Hector J. Cuellar
Managing Director
Area/Industries Manager
Bank of America

Ronald A. Erickson
Chief Executive Officer
Holiday Companies

Ray L. Hunt
Chairman of the Board
Hunt Oil Company

Kenneth L. Lay
Chairman of the Board
Enron Corp.

* Eugene E. Habiger , Director, Office of Security and Emergency Operations, served until January 2001.

David L. Lemmon
President and
Chief Executive Officer
Colonial Pipeline Company

John H. Lichtblau
Chairman and
Chief Executive Officer
Petroleum Industry Research
Foundation, Inc.

Steven L. Miller
Chairman, President and
Chief Executive Officer
Shell Oil Company

James J. Mulva
President and
Chief Executive Officer
Phillips Petroleum Company

Richard B. Priory
Chairman and
Chief Executive Officer
Duke Energy Corporation

Daniel Rappaport
Former Chairman of the Board
New York Mercantile Exchange

Lee R. Raymond
Chairman, President and
Chief Executive Officer
Exxon Mobil Corporation

Richard E. Terry
Chairman and
Chief Executive Officer
Peoples Energy Corporation

Gerald Torres
Associate Dean for Academic Affairs
University of Texas School of Law and
Vice Provost
University of Texas at Austin

C. L. Watson
Chairman of the Board and
Chief Executive Officer
Dynegy Inc.

Daniel H. Yergin
President
Cambridge Energy Research Associates

COORDINATING SUBCOMMITTEE OF THE NPC COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

CHAIR

Charles E. Dominy
Vice President
Government Affairs
Halliburton Company

GOVERNMENT COCHAIR

Paula L. Scalingi
Director
Office of Critical Infrastructure Protection
U.S. Department of Energy

ASSISTANT TO THE CHAIR

Forrest L. Carpenter III
Cyber Security Consultant
Global Information Services
Texaco Inc.

SECRETARY

Marshall W. Nichols
Executive Director
National Petroleum Council

* * *

Raymond W. Bergeron
Manager
Corporate Security
Shell Oil Company

M. Frank Bishop
Executive Director
National Association of
State Energy Officials

Thomas D. Carmel
Corporate Counsel
Conoco Inc.

Donald M. Field
Executive Vice President
Peoples Energy Corporation

Bobby R. Gillham
Manager
Global Security
Conoco Inc.

Lawrence J. Goldstein
President
Petroleum Industry Research
Foundation, Inc.

Michael C. Hicks
Manager
Corporate Security
Enron Corp.

Thomas R. Holland, Jr.
Manager
Corporate Security – Worldwide
Phillips Petroleum Company

Kevin J. Lindemer
Senior Director
Refined Products and
Global Downstream
Cambridge Energy Research Associates

David J. Manning
Senior Vice President
Corporate Affairs
KeySpan Energy

James R. Metzger
Vice President and
Chief Technology Officer
Texaco Inc.

Rolando D. Moss
Senior Director
Corporate Security
Dynegy Inc.

A. R. Mullinax
Senior Vice President
Global Sourcing and Logistics
Duke Energy Corporation

Catherine A. Travis
Director
Information Security
Questar Corp.

Vic A. Yarborough
Vice President Technology
Colonial Pipeline Company

SPECIAL ASSISTANTS

W. R. Finger
President
ProxPro, Inc.

Ronald E. Fisher
Deputy Director
Infrastructure Assurance Center
Argonne National Laboratory

Joseph S. Gurga
Manager
Program Office
Information Technology Services
Peoples Energy Corporation

John H. Guy, IV
Deputy Executive Director
National Petroleum Council

John R. Johnson
Principal Advisor
Shell Services International

Stuart L. Schertz
Manager
Security Services
Shell Oil Company

Curtis R. Smith
Manager
Information Security
Conoco Inc.

Richard D. Vance
Strategic Business Consultant
Duke Energy Corporation

Peter van de Gohm
Director
Information Assets Protection
Enron Energy Services

Acronyms and Abbreviations

B2B	business to business
CCPS	American Institute of Chemical Engineers' Center for Chemical Process Safety
CIAO	Critical Infrastructure Assurance Office
CIP	critical infrastructure protection
CIRP	Cyber Incident Response Plan
CDC	Centers for Disease Control
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
e	electronic
EEI	Edison Electric Institute
EIA	Energy Information Administration
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
EU	European Union
FBI	U.S. Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FOIA	Freedom of Information Act
FS/ISAC	Financial Services Information Sharing and Analysis Center
GRI	Gas Research Institute
G8	Group of Eight industrialized economies: Britain, France, Germany, Japan, United States, Italy, Canada, and Russia
IEA	International Energy Agency
IEC	International Electrotechnical Commission
ISAC	Information and Sharing Analysis Center
ISO	International Standards Organization
IT	information technology
IT/ISAC	Information Technology Information Sharing and Analysis Center
ITAA	Information Technology Association of America
LLC	Limited Liability Company
LNG	liquefied natural gas
LPG	liquefied petroleum gas
MEMS	Mutual Emergency Materials Support
MOU	Memorandum of Understanding
MSWT	Multisensor and Warning Technologies
NAFTA	North American Free Trade Association
NASA	National Aeronautics and Space Administration
NCC	National Coordinating Center for Telecommunications
NERC	North American Electric Reliability Council
NIPC	National Infrastructure Protection Center
NPC	National Petroleum Council
NTSB	National Transportation Safety Board
OCA	offsite consequence analysis
OPS	Office of Pipeline Safety
PDA	Personal Digital Assistant
R&D	research and development
RMP	risk management plans
SCADA	supervisory control and data acquisition
SPR	U.S. Strategic Petroleum Reserve
Y2K	Year 2000

National Petroleum Council
1625 K Street, NW
Suite 600
Washington, DC 20006

recycled
paper