E-Commerce Vulnerabilities: Impacts on the Transportation System

Background Paper

Volpe National Transportation Systems Center

Research and Special Programs Administration

March 2002

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

In the aftermath of the September 11, 2001, terrorist attacks, security experts have braced themselves for cyber attacks: "We concluded that cyber attacks immediately follow physical attacks within the circumstances of the political conflicts," commented a former chief of the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center.[1] Earlier that week, another former intelligence officer at the Department of Defense (DOD) warned that the United States needed to prepare for an "electronic Pearl Harbor;" while a retired Air Force general stated, "I would suspect a cyberattack would be next, and that would be absolutely paralyzing."[2]

At the same time, the Atlanta-based Internet Security Systems Inc., which operates the Information Sharing and Analysis Center (ISAC) – established at the direction of Presidential Decision Directive (PDD)-63 – placed its operations center on what it calls AlertCon 3 (with the highest level being AlertCon 4) in order to focus information technology (IT) security efforts on the potential for – and defense against – an Internet component to the terrorist attacks.

This background paper outlines the elements of emerging vulnerabilities in today's information – or cyber – systems supporting electronic commerce in transportation. The paper creates a framework to address system threats and vulnerabilities through sequential processes of risk assessment, risk management, and risk communication. The framework will serve as a point of reference for upcoming analyses of transportation cyber vulnerabilities.

What are the risks of cyber terrorism? In September 2001, the U.S. General Accounting Office (GAO), issued a report titled *Combating Terrorism: Selected Challenges and Related Recommendations.* It found:

> With the coordinated terrorist attacks against the World Trade Center in New York City and the Pentagon in Washington, D.C., on September 11, 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas...The initial step toward developing a national strategy is to conduct a national threat and risk assessment...Regarding risks to computer systems and, more importantly, to the critical operations and infrastructure they support, an array of efforts has been undertaken...but independent audits continue to identify persistent, significant information security weaknesses that place Federal operations at high risk of tampering and disruption....[Furthermore,] substantive analysis of sector-wide and cross-sector interdependencies and related vulnerabilities has been limited...GAO recommends developing a more detailed strategy for combating computer-based attacks, which should be linked to a national strategy to combat terrorism.[3]

In support of the GAO call for a national threat and risk assessment, this paper proposes a process for identifying the national IT assets, their vulnerability to disruptive threats, the consequences of disruption, and effective countermeasures.

Creating a Framework for Risk Analysis

In this paper, the following definitions apply:

Risk is the likelihood that a threat will harm an asset with some severity of consequences.[4] Not all hazards have severe enough consequences to warrant remedial action. Risk analysis considers the likelihood that an unwanted event (due to an internal failure or external act) will occur and the likelihood that the occurrence will have an impact with some degree of severity. The impact of the unwanted event represents the consequences – including death, injuries, economic losses, environmental damage, or no significant loss or damage – expressed in monetary or non-monetary terms. Mitigation efforts will focus on consequences deemed unacceptable.

Risk control refers to actions taken to reduce the effects of unwanted incidents or threats. The process of assessing the probable threats, and devising strategies to control damage and mitigate the adverse consequences is addressed under the broad umbrella of risk analysis.

Risk analysis is used here as "an approach to risk control that permits assessment and management of risk to an individual or an organization due to hazards, deleterious effects, and damage to property."[5]

Risk assessment is the process of synthesizing information about a potentially hazardous situation, and includes an overview of the underlying contributing factors, the existing vulnerabilities, the exposure of the industry segments, and the potential consequences. To this extent, risk assessment is not about finding a single remedy or technology fix, but rather preparing the groundwork for informed decision making.[6]

Risk management is the process of understanding risk and deciding on and implementing actions to reduce it. It involves a process of determining acceptable risk – i.e., a level of risk from an unwanted event or threat deemed to be sufficiently low to enable the activity to be instituted or continued – so that risk mitigation strategies can concentrate on deployment of countermeasures for unacceptable levels of risk. In this respect, risk management is an iterative process of analysis, deliberation, and evaluation that arrives at risk mitigation decisions through a consensus building process.

Risk communication consists of the process of information exchange among the industry and the government sectors. It also includes evaluation of the policy options and effective implementation of regulatory measures.

The risk analysis framework for this paper is laid out in Figure 1 and emphasizes four major steps: risk assessment, risk characterization, risk management, and risk communication.[7]

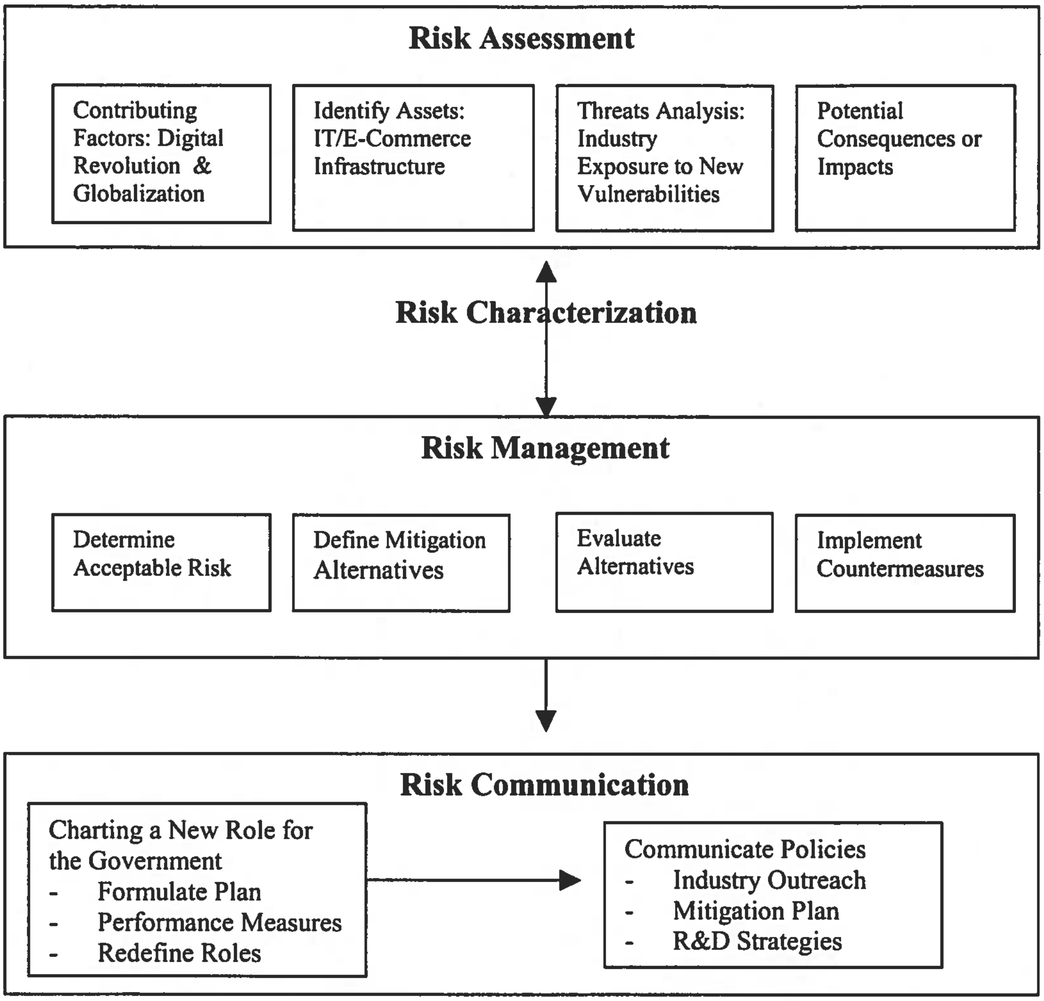

Risk Assessment
Contributing Factors: Digital Revolution & Globalization
Identify Assets: IT/E-Commerce Infrastructure
Threats Analysis: Industry Exposure to New Vulnerabilities
Potential Consequences or Impacts
Risk Characterization
Risk Management
Determine Acceptable Risk
Define Mitigation Alternatives
Evaluate Alternatives
Implement Countermeasures
Risk Communication
Charting a New Role for the Government
- Formulate Plan
- Performance Measures
- Redefine Roles
Communicate Policies
- Industry Outreach
- Mitigation Plan
- R&D Strategies

Figure 1. Risk Analysis Framework

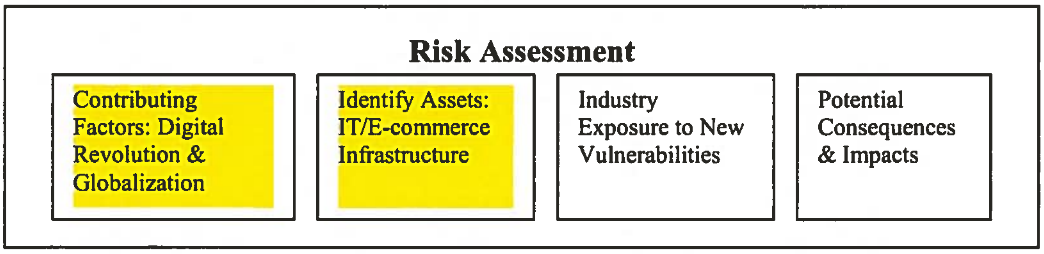
This paper will focus on risk characterization: linking risk assessment to risk management and risk communication, and identifying the economic and technological forces underlying the emerging vulnerabilities.

- ❑ Section 2 expands the risk assessment process by identifying the macro-level national IT assets.
- ❑ Section 3 completes the risk assessment process by reviewing the threats and vulnerabilities in cyber systems, the potential consequences – e.g., disruptions in system availability, integrity, or confidentiality — of their exploitation.
- ❑ Section 4 examines risk management issues relating to determination of acceptable and unacceptable risks and the creation of a risk matrix.
- ❑ Section 5 examines the risk management issues relating to the evaluation of mitigation alternatives and countermeasures.

In order to reduce and control cyber vulnerabilities, the following steps are recommended:

- **Identify the assets of the IT and e-commerce infrastructure.**
- **Identify vulnerabilities of the cyber-based economies and IT systems.**
- **Identify and rank cyber threats and identify consequences of a cyber attack.**
- **Create risk management framework by determining acceptable risk, evaluating risk mitigation options, and implementing countermeasures.**

2. IDENTIFYING THE ASSETS: THE DIGITAL ECONOMY



Risk Assessment

Contributing Factors: Digital Revolution & Globalization

Identify Assets: IT/E-commerce Infrastructure

Industry Exposure to New Vulnerabilities

Potential Consequences & Impacts

In order to address areas of vulnerability and impacts of potential attacks, the relevant assets of IT and e-commerce must first be identified. The infrastructure is characterized by the following:

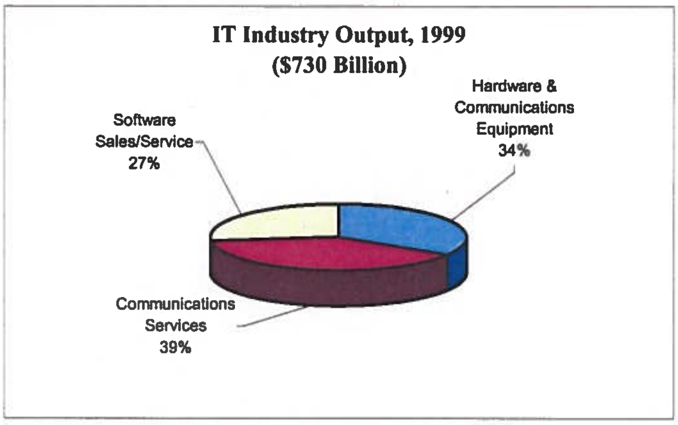
- IT industry revenues totaled $730 billion in 1999, or roughly 10 percent of the GDP, in 6 IT-intensive sectors:
  - Telecommunications
  - Semiconductor manufacturing
  - Computer manufacturing
  - Securities
  - Wholesale
  - Retail

- Positive characteristics include:
  - Decentralized corporate and IT controls
  - Distributed communications
  - Open interoperable communications systems
  - Collaborative venues and shared networks
  - Adaptive, flexible, and intelligent systems

2.1 Scope of Assets: IT Systems Claim a Growing Share of the Economy

> "The newest innovations, which we label information technologies, have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even five years ago."
> Alan Greenspan, Chairman, Federal Reserve Board, May 6, 1999

As shown in Figure 2, estimates of commercial IT revenues vary widely, depending on how IT revenues are defined. The Department of Commerce (DOC) has reported that IT sector revenues in 1999 totaled $730 billion.[8]



Source: DOC, *The Emerging Digital Economy II*, 1999.

Figure 2. IT Industry Output, 1999

IT has been credited with fueling the tremendous economic growth that lasted through most of the 1990s. Earlier this year, Alan Greenspan credited declining IT prices – and more competitive markets – for slowing down threats of inflation because of "the lack of pricing power."[9] The industry output took off in the early 1990s. The overall share of IT in the economy is growing, rising from 4 percent of the GDP in 1977 to more than 10 percent today. (For more detail, see Figures A-1 and A-2.)

IT contribution to GDP growth has risen steadily over the past decade. In 1992, IT accounted for less than 14 percent of the GDP growth; by 1999, close to 35 percent of the GDP growth was attributed to IT (see Figure A-3). Contribution of IT to business equipment investment is also significant. Computers, as a share of investment in producers' durable equipment, rose from 7.75 percent in 1990 to 45.7 percent in 1998,[10] while computing costs plummeted at exponential rates, approximately 25 percent per year. (For more detail, see Figure A-4.)

IT has also begun to show up in some productivity statistics. From 1995 through 2000, the nation's overall productivity rate grew at a 2.5 percent annual rate (contrasted with an annual productivity growth rate of 1.4 percent for 1972 through 1995). Nearly all the productivity gains have been in six IT-intensive sectors of the economy: telecommunications, semiconductors manufacturing, computer manufacturing, securities, wholesale, and retail.

The multiplier impact of IT is far greater than the direct revenues. IT's total economic impact goes beyond the direct revenues generated. Economic Impact Assessment for IT systems can be conducted by using quantitative methods, including econometric/regression modeling, that assess the direct and indirect impacts of the systems.[11]

2.2 Positive Characteristics

Today's cyber economies benefit from interconnected IT networks and infrastructure characterized by:

Decentralized corporate and IT controls. As corporate locations have been decentralized, so have their IT systems. With the dispersal of the domestic economy to the periphery and trends in outsourcing and globalization of production, the old centers of control – supported by powerful IT systems – have changed their function and focus.

Distributed communications. Network connectivity is no longer associated with a physical connection. Distributed IT systems have moved communications control to individual users. These distributed control and communications have, to some extent, reduced vulnerability to large-scale threats.

Open interoperable communications systems. Wireless communication systems are coming into widespread use. By one estimate, there will be 175 million wireless users in the United States by 2005. It is also estimated that most of the globe will be accessible to high-bandwidth space-borne links, and that by 2010, all populated areas in developed countries will be covered with multiple, competing surface systems.

Collaborative ventures and shared networks. An increasing number of corporations are forming alliances and relying on shared databases that, while generating significant cost savings, tend to increase vulnerabilities. U.S. automobile manufacturers, for instance, have a shared electronic system for supply purchase. Automakers have also formed close alliances with transportation carriers. For example, General Motors partners with FedEx to manage its inventory delivery. Ford Motor Company and the United Parcel Service have formed a strategic alliance for delivery of vehicles from Ford plants to dealers and customers in North America.

Adaptive, flexible, and intelligent systems. Today's cyber technologies have enabled manufacturers and suppliers around the world to manage their supply chains more efficiently by transforming logistics operations into flexible, adaptive, and intelligent systems; i.e., pull logistics. Defined as the production process driven by actual sales rather than demand forecasts, pull logistics allows production decisions to center on the replenishment of sold inventory, instead of the production of likely-to-sell stock, through access to electronic data.[12] A pull-based supply chain integrates the production planning and design processes with the logistics of distributing products.

Wal-Mart, the quintessential pull-driven retailing giant, has cut its logistics cost by sending point-of-sale data to all its vendors and replenishing store supplies twice a week, without goods ever "sitting in inventory." Dell Computer, another practitioner of pull logistics, has eliminated most of its finished-goods inventory and bypassed many of its supply chain intermediaries through the control of information flow. Information is substituted for inventory, and inventory ships only when there is a demand from a real end-consumer. American automakers also practice pull logistics as a solution to mounting competitive pressures. They are shifting from a supply chain where they push inventory to dealerships to one where consumers pull products.

Advanced IT systems are integral to pull-based production, enabling businesses to manipulate an array of timely market and shipment data in real time. For example, Schneider National, a leading trucking firm, is an industry leader in deployment of advanced technologies to provide full in-transit visibility for its fleet and containers. For some years, the trucking firm has been using Global Positioning System (GPS), Electronic Data Interchange (EDI), and automated order processing systems to manage loads and truck fleet.

Customized merchandizing is another facet of today's production and logistics networks. Mass customization and the built-to-order production methods combine the production efficiency of mass-produced goods with the customer-focused quality of a master craftsman. By one estimate, roughly 60 percent of U.S. production and sales today are processed to order rather than to stock. Motorola, for instance, manufactures pagers in a single plant in up to 29,000 varieties, in lot sizes as small as 1 unit. Automated design and order processing allows Motorola to design each customer's pager on a sales agent's laptop, sending specifications to the factory to produce and deliver the products on demand.

The value of today's intelligent, adaptive IT networks is due partly to feedback systems. Information has become a more valuable asset in today's logistics network because it can be spread simultaneously through an entire network – rather than in a linear, sequential manner – with feedback from intelligent agents imbedded in the system. Businesses are increasingly helped by technologies that support "bots" and autonomous network agents; i.e., software entities that conduct information retrieval and other business on behalf of network users. These intelligent agents have "recursive effects," that is, they are guided by stored-program devices that define their own instructions and goals.[13]

2.3 Components of the IT infrastructure in Transportation

To identify vulnerabilities, the transportation-relevant components of IT assets must be identified. IT infrastructure includes computer hardware, software, and communications equipment and services.

The components of the IT infrastructure in transportation applications are as follows:

Computer Hardware
Mainframe automated accounting systems and minicomputers, EDI, personal computers, and EDI for computer-to-computer exchange of routine business information in standard data format are included in this category.

Telecommunications Networks
Increasingly, the structure of the nation's telecommunications networks is changing from stand-alone computers, or plain old telephone service supported by copper landlines, to interconnected networks of computers and communications services supported by wireless cellular, cable, and fiber optics networks. Networks are formed when communications devices tie a group of computers together. They can be tied into a local area network (LAN) with physical wires in small areas such as a building, or across a larger area or corporate compound into a wide area network (WAN). Networks can be formed by dedicated phone lines (Integrated Services Digital Network or DSL), dial-up connections, fiber optic, or through an electromagnetic connection such as radio links or microwaves. Voice, FAX, computing, and video entertainment are now blended with real-time communication services previously offered by phone companies, and can be loaded onto public data networks instead of using dedicated systems.

The Internet
The Internet encompasses all facets of communications, information software, and computing equipment. Migration of services to the Internet is a significant recent trend affecting cyber infrastructure capacity. For cost and marketing purposes, a growing number of services are migrating to the Internet. This is consistent with the growing trend of user control over the contents of the networks. Services such as banking, financial services, medical information, and law enforcement are migrating onto the Internet, allowing individual and corporate customers to interact with their accounts and initiate activities over the public data networks.

Migration to the Internet also is eliminating some supply-chain intermediaries through a process referred to as "disintermediation," enabling businesses to conduct production or marketing transactions directly on the Web. One consequence of the migration is the increasing consolidation within many of the migrated services. As new interoperability protocols are developed, disparate service providers are able to consolidate. These trends have potential impacts on system vulnerability.

GPS and Remote Sensing (RS) Technologies
In addition to use for air traffic control and navigation in aviation, rail, transit, marine, and highway transportation rely on GPS services. Advanced rail freight technologies for positive train control involve

application of digital data communications, automatic positioning systems, including Differential GPS (DGPS), trackside interface detectors, and on-board computers to manage and control rail operations. For marine navigation, the U.S. Coast Guard has installed DGPS every 200 miles along the coast and major rivers to allow ships equipped with GPS equipment to identify their position within 5-10 meters. Freight and passenger highway and transit services also use GPS extensively.

RS technologies consist of several types of GPS, aerial imaging, and near-earth terrestrial data platforms. These technologies use sensors to collect data and generate photographic or digital images for end-uses including land-use change detection and 3D modeling. A National Aeronautics and Space Administration and Department of Transportation (DOT) partnership currently explores RS applications in traffic surveillance and monitoring; infrastructure asset management; and hazardous materials spills/disaster mitigation.

Intelligent Transportation Systems

Integrated ITS programs have been deployed in 78 of the largest metropolitan areas in the United States.[14] Since 1997, DOT has been tracking the progress in deployment of ITS programs for nine infrastructure components. The nine components of the infrastructure are as follows:

- Freeway Management
- Arterial Management
- Incident Management
- Emergency Management
- Transit Management
- Electronic Toll Collection (ETC)
- Electronic Fare Payment
- Highway Rail Intersections
- Regional Multimodal Traveler Information

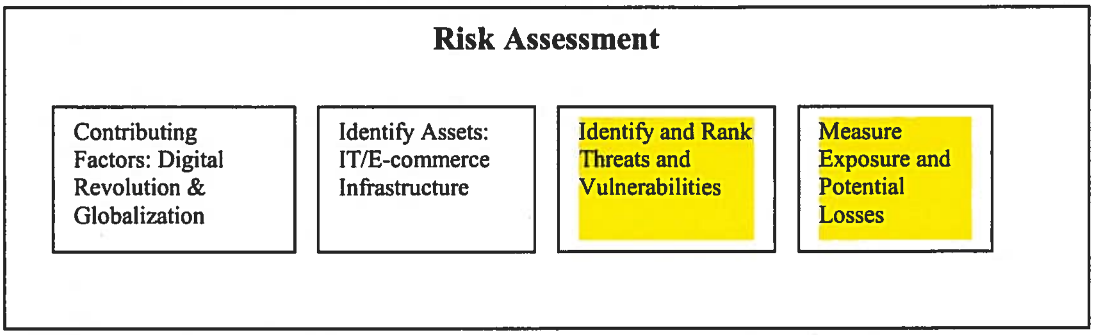
Table 1 summarizes ITS deployment for FY 2000.

Table 1. FY 2000 ITS Deployment Summary

ITS Component	Percent Metropolitan Areas
Freeway miles with real-time traffic data collection technologies	51%
Freeway miles covered by on-call service patrols	51%
Arterial miles covered by on-call service patrols	6%
Signalized intersections under centralized or closed loop control	70%
Toll collection lanes with ETC capability	81%
Fixed-route transit vehicles equipped with AVL	85%
Fixed-route buses accepting electronic fare payment	58%
Highway-rail intersections under electronic surveillance	22%
Emergency management vehicles under computer-aided dispatch	90%
Freeway conditions disseminated to the public	22%

Source: ITS Joint Program Office, Tracking the Deployment of the Integrated Metropolitan Intelligent Transportation Systems Infrastructure in the USA: FY 2000 Results, July 2001.

3. IDENTIFYING VULNERABILITIES, THREATS, AND RISKS



Risk Assessment

Contributing Factors: Digital Revolution & Globalization

Identify Assets: IT/E-commerce Infrastructure

Identify and Rank Threats and Vulnerabilities

Measure Exposure and Potential Losses

This section will continue the creation of the risk assessment framework through the following steps:

- **Identify vulnerable assets**
- **Rank mission critical threats**
- **Identify threats**
- **Estimate potential losses and impacts**
- **Estimate exposure levels**

3.1 Identify Vulnerable Assets

Vulnerabilities are defined as "physical, technical, administrative, procedural, or human related characteristics of an asset that affect the difficulty of a specific attack being successful in causing a loss."[15] Four factors are considered when determining asset vulnerability:

- Ease of access
- Level of effort and knowledge required
- Existing security measures
- Degree of control by attackers over outcomes

The pervasiveness of today's cyber systems have placed new constraints on risk management and risk policies communication:

- Ensuring secure access has become harder with the distributed communications systems and decentralized controls.
- Minor malfunctions in shared networks – proliferated with the rise of collaborative ventures – can potentially lead to cascading losses.
- Adaptive and intelligent systems have engendered feedback effects not foreseen by the initial system designs and led to greater system instability.
- Interdependence among systems has made it more difficult to assign responsibility and manage risk.

The factors contributing to greater vulnerability of the national critical infrastructure, according to the PCCIP commission report in 1997, include proliferation of new access points, more remote control for operations and maintenance, and less control due to greater prevalence of foreign ownership. The report also cited the broader population of insiders, the growing rate of open source communications, and insufficient physical and cyber security planning as reasons for higher incidences of security breaches.[16] The growing number of techniques available to penetrate, gain access, or alter IT systems have also created greater opportunities to disrupt, deny access, destroy, or distort the contents of IT systems or documents.

Three broad areas of cyber system vulnerability emerge from the juxtaposition of the National Institute of Standards and Technology's (NIST) five threat categories and the trends in cyber systems reviewed in Section 2:

- Service availability is threatened by system interdependence.
- Content integrity is threatened by distributed and decentralized systems.
- Data authenticity/confidentiality is threatened by open and adaptive commercial networks.

3.1.1 Service Availability: System Interdependency Risks

Significant vulnerabilities emerge from interdependence among system components and complex inter-linkages. Charles Perrow has defined high-risk interdependent systems as those characterized by system complexity and tight coupling.[17] System complexity is characterized by:

- Tight spacing of equipment
- Proximate production steps
- Many common mode connections of components not in production sequence
- Limited isolation of failed components
- Specialized personnel with limited awareness of interdependencies
- Limited substitution of supplies
- Unfamiliar or unintended feedback loops
- Many control parameters with potential interactions
- Indirect or inferential information sources
- Limited understanding of some processes

Subsequent to the September 11, 2001, destruction of the World Trade Center, the near-catastrophic outcomes of such interlinkages were demonstrated by the loss of telecommunications services, which, in turn, impeded financial service transactions and delivery of electric power. John Tritak, Director, Critical Infrastructure Assurance Office, in a testimony before a senate committee, pointed out the disruptive effect of this interdependence: "The cascading fallout from the tragic events of September 11 graphically makes the business case for critical infrastructure protection. That the loss of telecommunications services can impede financial service transactions and delivery of electric power is no longer an exercise scenario."[18]

Service availability is also threatened when the growing economic and sector interlinkages create what some reports refer to as a "system of systems," where "everyone is a customer," as illustrated in the box below in the case of the AT&T network failure of September 21, 1991.

The growing reliance on public networks also threatens service availability. Migration to public networks is growing in all facets of today's IT infrastructure. Infrastructure providers such as power companies and public utilities are employing the public data networks to transmit their monitoring and control information, instead of using private circuits. This migration is helped by the *de facto* standards design and process definitions that are enabling linkages among public and private networks. This migration is likely to expose utility companies to new network-based threats.

Threats to service availability may also come through new vulnerabilities created in the realm of remote access and space-based navigational systems. With the disappearance of the government monopoly on space-borne intelligence gathering, RS technologies – especially satellite imaging – are becoming cheaper and more widely available. As imaging technology gets better, it is likely that it can become a target for adversaries, making power, water, railroad, farming, and some facets of the telecommunications industry vulnerable. The DOT study on the vulnerabilities of the transportation systems relying on GPS recently concluded that the signals can be blocked or jammed, or the satellites themselves can be attacked.[19]

On September 17, 1991, a power failure at the AT&T switching center in lower Manhattan disrupted AT&T 1-800 service for 8 hours, resulting in the blockage of 5 million calls. Losses were estimated at hundreds of million of dollars. The incident began at 10:00 A.M. when AT&T switched to its own power – based on an agreement with New York's Consolidated Edison Power Company, that on warmer days, when the Edison facilities are heavily loaded – AT&T would do so. The incident occurred due to the failure of some power equipment and alarm systems that went undetected.

- The direct costs to AT&T were $760,000 to $1 million (including disrupted operations, revenue loss, investigations, public relations needs, increased vigilance).
- Losses to air travelers: $4.8 million (affecting 85,000 passengers, with 688 hours of delay) because the Federal Aviation Administration leased private lines from AT&T to interconnect airports with the New York Air Traffic Center in Long Island.
- Costs to airlines due to air traffic disruptions: $9-17 million (635 delayed flights and 658 cancelled flights)
- Business losses to brokerage operations: ranging from hourly costs up to $10.8 million (including credit card authorizations, catalog sales, airline reservations, tele-ticket sales, package shipping, automated teller machine fees, etc.).

The report estimated the total losses as more than $100 million to the customers "because of the difficulty in estimating the numbers of individuals and businesses affected by the outage, revenues foregone are conservatively estimated in the hundreds of millions." One of the largest "victims" of AT&T was the airline industry, who had to cease operations because control towers could not communicate with each other. The 100:1 cost differential between the direct losses to the facility suffering a service disruption, and the losses to the corporate customers illustrates the powerful cascading effects of interrelated businesses. The more than 100-fold increase in downstream costs to the customers is a testimony to the applicability of the concept of a "nation where everyone is somebody's customer," a fact that influences the size of the potential losses as well as uncertainties. The report maintained that a byproduct of such interdependence is the emergence of a vast nation of "customers" of other infrastructure. So entire infrastructures, banking, transportation, manufacturing, healthcare, and even government – are customers of other infrastructures – and all with strong expectations of "entitlement" to availability and reliability of services, the report stated. One effect of this trend on the system vulnerability is that individual businesses are less likely to have adequate awareness of the risks or incentive to implement the needed security measures.

Source: Report to the President's Commission on Critical Infrastructure Protection, *Economic Impacts of Infrastructure Failures*, 1997.

Another area of vulnerability, with respect to service availability, is on the nation's Advanced Traffic Management System (ATMS). This vulnerability was assessed for a cyber attack scenario in a city with an established ATMS and deployed to improve throughput. In this scenario, a computer hacker discovers a security breach in the ATMS Internet connection designed to provide real-time traffic information to the public. The hacker then introduces a virus that corrupts the computer files that run the ATMS.[20]

Similar vulnerabilities in supervisory controls and data acquisition (SCADA) systems threaten service availability in the nation's pipelines. One report constructed a cyber attacks scenario on SCADA, based on the premise of penetration of the SCADA computer center through the corporate computer network. The intruder plants a computer virus into the SCADA system, corrupting program files. The SCADA produces unpredictable results and is rendered inoperable. Operations must be conducted remotely, using telephone communications to provide direction to operations personnel at remote facilities. This results in increasing safety margins, which in turn reduces the flow of gas through the line.

Threats to service availability in the rail industry are also related to the interconnections in the industry. Rail industry consolidation and inter-connected communication, dispatching, and business-critical database functions have placed these systems at greater risk of cyber-attack and exploitation. Customer-driven focus on web-based shipment tracking, just-in-time delivery, cross-border mergers, and increased dependence on electronic commerce and data exchange, have all raised the vulnerability of the railroad industry to cyber attacks.

3.3.2 Content Integrity: Distributed Control Risks

Along with the growing practice of networking, new risks associated with the decline of network integrity have emerged. The pervasive application of IT networks in telecommunication, banking, energy and utilities, and transportation poses new threats on system integrity. With open access for trade and a distributed location of control for decentralized communications networks, it is increasingly difficult to assert adequate levels of control over transactions. As new systems are being integrated on top of one another, a system that is failsafe one day can become a loophole the next. The ability to network has outpaced the ability to protect networks.

With the growth of wireless services, the structure of the telecommunications infrastructure has changed. The new infrastructure allows customers to participate in administration of the media they utilize. Peer-to-peer networks today allow the customer control of content and even bandwidth. Internet service providers (ISPs) are allowing more businesses and individuals to regulate and control the bandwidth they pay to use. This decentralization trend is inevitable as customer requirements diversify and competition among providers intensifies.

Some industry analysts have maintained that in the aftermath of the Telecommunications Act of 1996, network integrity has been compromised. The distributed control of the telecommunications infrastructure has opened up new vulnerabilities to disruption, opportunities for fraud, service theft, and outright denial of service. Virtual links (i.e., network connections defined by digital codes as opposed to physical wiring plans) have connected many users to machines. Faster computer processors are now supporting a growing traffic for the new and powerful information appliances in the home and office, aircraft, trains, and automobiles. With increased distributed intelligence, the demarcation of the network boundary and the user's space is blurred. One policy implication of this shift, is that increased competition for service offerings encourages *de facto* interconnections to public and private networks. This allows providers to offer users choices among technologies, carriers, rates, tariffs, and services, but also creates new vulnerabilities.[21] Pervasive application of wireless devices such as Bluetooth and wireless standards like 802.11b illustrate the challenges arising from today's cyber technologies. Information integrity and privacy concerns about the proliferation of these devices are significant. Though the devices are equipped with wireless encryption, many facilities do not turn on the encryption system included with the software to protect broadcast data integrity.

3.3.3 Data Authenticity/Confidentiality: Open Access Risks

The transition to an open digital infrastructure has led to a distributed computer network, allowing greater user control. With the user performing some of the carrier functions and sharing control over routing, bandwidth allocation, and administration, new vulnerabilities are emerging. This open infrastructure has superimposed a new system over the old one, creating a heterogeneous system with hybrid protocols and standards. The layered functions performed in the new digital infrastructure, as one analyst has noted, are analogous to running a train that could accommodate a steam, diesel and electric engine equally well, and each passenger and freight car could be manufactured by different techniques and owned by different companies.

The risks of data confidentiality over the Internet are significant. The Internet was not designed for secure commercial use. When DOD's Defense Advanced Research Project Agency initiated the Internet in 1969, it was designed to connect different types of computers across geographically dispersed areas. It was intended as a communications system that could continue to operate even if one part was disabled. Its very design centered on openness and the sharing of information among scientists and researchers. The open communications protocol the Internet was built on – known as TCP/IP – utilizes multiple alternative pathways to achieve an extremely high degree of resilience. The robustness of the Internet – its lack of security notwithstanding – was put to the test on September 11, 2001. The system proved a valuable service when the communications lines in Manhattan were disrupted.

The risks and benefits of the new telecommunications infrastructure should be viewed together. On the one hand, the broadened reach of IT in the economy has allowed telecommunications services to diversify not only as a competitive strategy but also as a defense against large-scale attacks. This diversity has protected users from catastrophic disruption. Businesses no longer put all their telecommunications needs in one basket. As new service providers enter the market and existing providers are able to offer broader ranges of service two things have happened. On the other hand, individual risks from focused attack are likely to rise as the trend toward offering any service over multiple media continues. Some analysts have suggested that the overall effect of this trend is likely to expose business and consumers to greater risks, as they "defocus" vulnerabilities by opening up more avenues for attack.[22]

Content control and confidentiality also is likely to get more difficult as data networks increasingly host other communication services. The boundaries between business sectors, based on their use of different media, are blurred. Loss of data privacy and confidentiality is highlighted by the problem posed by "record linkage," defined in a recent GAO report as a "computer-based process that combines multiple sources of existing data." For government agencies, benefits from these linkages have included informed policy debate, tracking program outcomes, and helping smaller public agencies with business planning. The downside is that record linkages often involve data on identifiable persons. As the report points out: "because the 'whole is greater than the sum of the parts,' linking independent data on individuals creates new information about them," violating privacy rights.[23]

3.2 Rank Mission Critical Threats

Not all cyber threats amount to an "electronic Pearl Harbor." Once cyber threats are identified, these threats must be ranked in order to determine where national resources are to be spent. The process would involve evaluating all potential threats, estimating the expected loss per incident and the expected number of incidents, and ranking each threat according to its risk.

3.3 Identify Threats

Identifying threats is useful only when it is based on a system that links threats to the risks they pose; i.e., the likelihood that the threat will harm an asset with some severity. Cyber threats encompass a wide range of actions that potentially can lead to the loss of one or more functionalities of the assets.

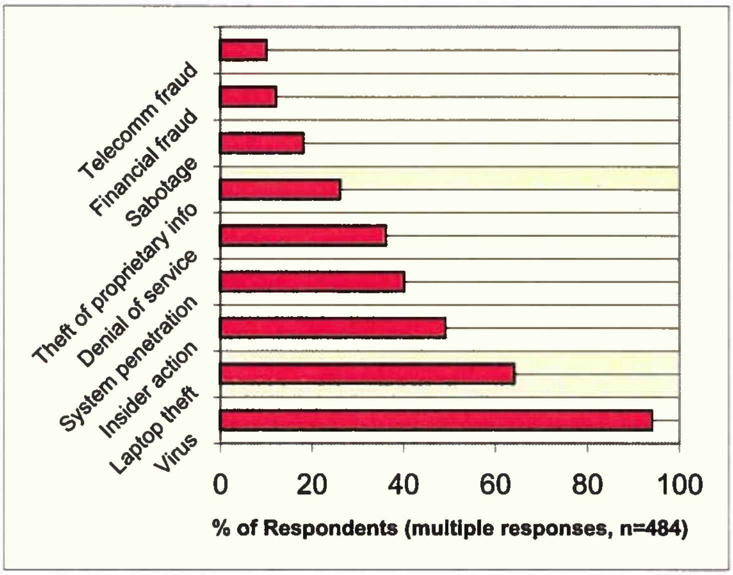
Threats need to be understood in the context of the perpetrators. Perpetrators range from thrill seeking hackers, lone criminals, and info-warriors to organized crime groups, malicious insiders, industrial spies, terrorists, and national intelligence organizations.

Threats include:

- **Criminal attacks**, including fraud, scams, destructive attacks, intellectual property theft, identify theft, brand theft, and prosecution difficulties.
- **Privacy violations**, including surveillance, invasion of networked database security, and traffic analysis of communication patterns.

- **National security threats**, including cyber terrorism, national intelligence, Netwars, and information warfare.[24]

Cyber threats range from incidents arising from blunders and the activities of "ankle biters" – recreational hackers with limited motives – to elaborate international warfare. Within a risk assessment framework, these threats are ranked with reference to the organizational mission of the agency conducting risk assessment. Figure 3 shows the percentage of the survey respondents reporting attacks or losses, as reported by the Computer Security Institute in 1998. Attacks relating to viruses and insider action were reported by more than 70 percent of the respondents.



Source: Computer Security Institute/FBI Computer Crime and Security Survey, March 2001.

Figure 3. Cyber Attacks or Abuse Detected by Survey Respondents

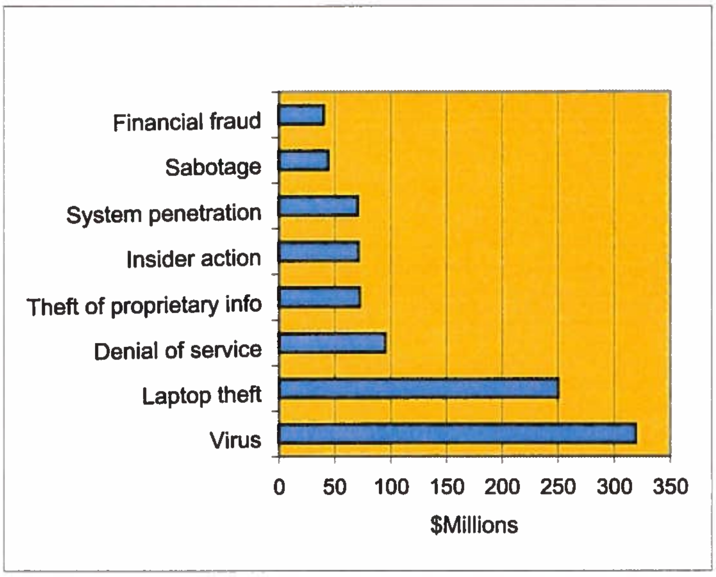
Cyber threats are generally directed against five interrelated, mission critical attributes of IT assets. As identified by NIST,[25] cyber attacks commonly pose threats to:

- System Availability: disruptions and destruction of service or system, including denial-of-service attacks.
- Data Integrity: unauthorized (malicious) or accidental modification of data; e.g., data insertion, deletion, and modification.
- Confidentiality: restricting access to the content of sensitive data to authorized individuals only. Security measures prevent the unauthorized *disclosure* of information.
- Authentication/Assurance: validity of a transmission, message, and data origin.
- Accountability/Non-repudiation: identification of the sender, and preventing an individual from denying that previous actions had been performed.

3.4 Estimate Potential Losses and Impacts

The full scope of cyber crimes and threats is not known. Only a fraction of the intrusions and crimes are reported, and less prosecuted. Therefore, assessing the potential impacts in terms of monetary losses is often difficult.

However, the reported losses from cyber attacks have been growing in magnitude and frequency over the past 5 years. In 2001, total reported losses amounted to nearly $400 million, 40 percent higher than those reported the previous year, and 3 times as large as the average of the past 3 years' losses. Financial losses reported due to attacks and intrusions in 1998 were highest for insider actions (including unauthorized access) and theft of proprietary information (discussed earlier in this section) (Figure 4).[26]



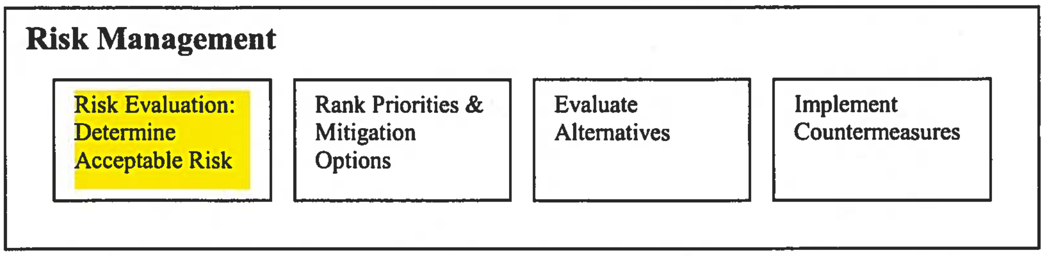
Source: Computer Security Institute/FBI Computer Crime and Security Survey, March 2001.

Figure 4. Financial Losses from Cyber Attacks

The Computer Security Institute survey of large corporations and government agencies – conducted with the participation of the FBI Computer Intrusion Squad – released a survey in March 2001 based on responses of 538 computer security practitioners:[27]

- 85 percent of the respondents detected cyber security breaches within the last 12 months.
- 65 percent acknowledged financial losses due to the computer breaches.
- 35 percent (186 respondents) were willing and/or able to quantify their financial losses, reported at $380 million.
- Losses showed a 40 percent increase over the 2000 reports, and a tripling of the losses over the average loss of $120 million in the 3 years prior to 2000.
- Most financial losses occurred through theft of proprietary information and financial fraud.

4. MANAGING THE RISKS: CREATING A FRAMEWORK FOR DETERMINING ACCEPTABLE RISK



Risk Management
Risk Evaluation: Determine Acceptable Risk
Rank Priorities & Mitigation Options
Evaluate Alternatives
Implement Countermeasures

Once the risk assessment process is complete and the vulnerabilities of cyber systems are identified, the next step is identifying how and by whom the emerging risk areas can be managed and monitored. This section reviews the elements of risk management, examining the evaluation process involved in determining acceptable risk and ranking priorities.

4.1 Framework for Evaluation: Determining Acceptable Risk

To successfully manage cyber risks, acceptable risk must be determined, and unacceptable risks must be managed by balancing the costs and payoffs.

How do organizations decide what levels of risk are acceptable? What is the acceptable level? Is the objective to reduce risk to zero levels? Who should bear the burden? Who decides what the risk tolerance level should be when the private and public sectors are so highly interdependent? What are the costs and consequences of doing nothing? Conversely, what are the payoffs?

To determine acceptable and unacceptable risk, the sequence of events leading to accidents, intrusions, or disruptions needs to be understood. Risk events may be the result of basic or root causes, such as inadequate knowledge, skills, or an organization's lack of a safety management system. Or they may result from immediate causes, such as failure to apply basic knowledge or unimpaired judgment. Often, an "error chain" is involved that leads to error cascades: a basic cause could lead to an immediate cause, and an incident, in turn, could trigger an accident. To mitigate risk, risk-reduction interventions need to be introduced at appropriate points in the error chain so as to prevent the cascading effect.[28]

The following two models evaluate acceptable and unacceptable risk.

Model 1. Not all risks require the same mitigation level. Along a continuum of acceptable-unacceptable risk – determined during the risk assessment phase – risk gradations can be established within a matrix. This matrix, adapted from the *Surface Transportation Vulnerability Assessment*[29] and depicted in Table 2, would enable a more efficient decision-making and resource allocation process. This risk creates four risk categories and accounts for both likelihood and severity. The highest priority, unacceptable risk, contains scenarios classified as Extensive Severity/High Likelihood.

The second risk category, undesirable risk, contains scenarios classified as:

- Extensive Severity/Moderate Likelihood
- Extensive Severity/Low Likelihood
- Moderate Severity/High Likelihood
- Moderate Severity/Moderate Likelihood

Risks that are acceptable with review include:

- Moderate Severity/Low Likelihood
- Minor Severity/High Likelihood
- Minor Severity/Moderate Likelihood

Minor Severity/Low Likelihood is categorized as an acceptable risk. This matrix represents scenarios in all modes and will enable a more efficient decision-making and resource allocation process.

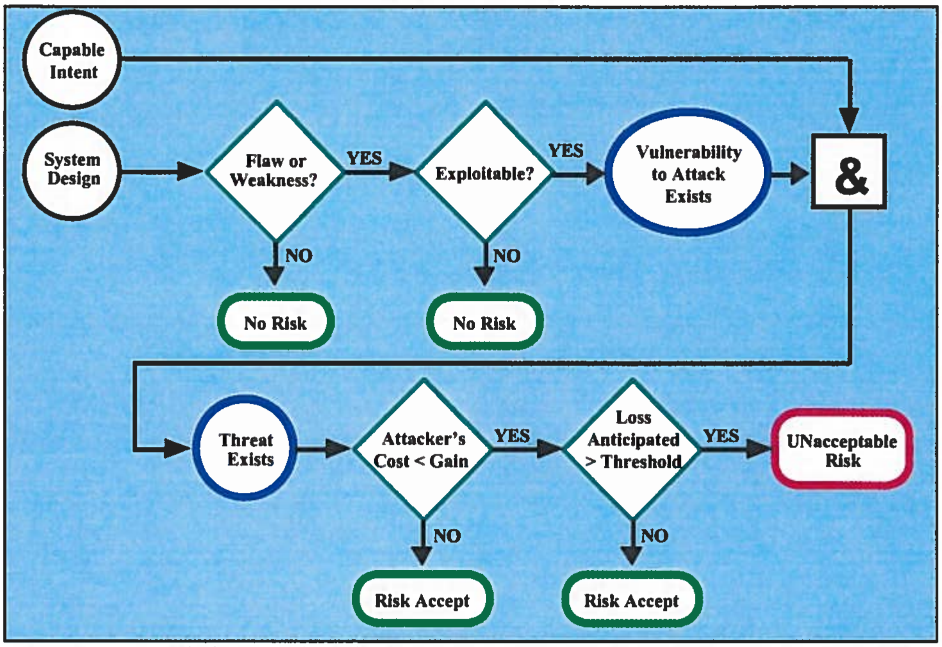
Table 2. Acceptable Risk Matrix

	Likelihood			Risk Categories
Severity	**High**	**Moderate**	**Low**	**A – Unacceptable** **B – Undesirable** **C – Acceptable with review** **D – Acceptable**
Extensive	A	**B**	**B**	
Moderate	**B**	**B**	**C**	
Minor	**C**	**C**	**D**	

Model 2. Another model for evaluating acceptable risks is the National Institute of Standards and Technology IT security model. NIST's model is designed to enable an organization to meet its mission objectives by implementing systems with "due care considerations of IT-related risks to the organization, its partners, and its customers."[30] An agency would undertake risk management to determine where technology capabilities are best applied. The elements of NIST's risk management are:

- Vulnerability assessment: identifying weakness in system security procedures, design, etc.
- Threat-source identification: identifying the intent and targeted method or the situation and method.
- Magnitude of threat: the potential for a "threat source" to exploit (intentionally) or trigger (accidentally) a specific vulnerability.
- Risk: the net mission/business impact (probability of occurrence combined with impact) from a particular threat source exploiting, or triggering, a particular IT vulnerability. Risk arises from:
  - Unauthorized (malicious or accidental) disclosure, modification, or destruction of information.
  - Non-malicious errors and omissions.
  - IT disruptions due to natural or man-made disasters.
  - Failure to exercise due care and diligence in IT implementation and operation.

The model then determines which risks are acceptable and unacceptable, as depicted in Figure 5.



Source: NIST, *Underlying Technical Models for Information Technology Security*, December 2001.

Figure 5. NIST's IT Security Model

5. EVALUATING MITIGATION ALTERNATIVES AND COUNTERMEASURES

> "We need to prevent disruptions; and when they occur, we need to make sure they are infrequent, short, and manageable. It is a technical challenge, because we must always remain one step ahead of the hackers."
> Governor Tom Ridge, Director, Office of Homeland Security, speaking of pervasiveness of the nation's information technology infrastructure.[31]

To be useful, the outcome of risk assessment should provide decision makers with information needed to make informed choices. In determining what type of security measures to deploy, asset owners need models that allow them to evaluate not only the risks but also the relative effectiveness of each countermeasure.

A national cyber security strategic plan must be formulated and implemented. Communication of this strategy will be aided by partnerships with the private sector.

As the economic and technological orders have changed, so have the rules of governance. Responding to Governor Ridge's charge "to prevent disruptions; and when they [do occur]...make sure they are infrequent, short, and manageable" requires a comprehensive risk control strategy based on risk assessment, risk management, and risk communication. Many agencies are currently in the process of formulating cyber security strategies.

Several recent GAO reports on information security risks have pointed out the need for a national strategy.[32] The findings of the National Advisory Panel to Assess Domestic Response Capabilities for Terrorism, formed by Congress in 1999 to assess the capabilities for domestic response to terrorism involving weapons of mass destruction, concluded that:[33]

- The United States has no coherent national strategy for combating terrorism.
- Cyber attacks inside the United States could have "mass disruptive," "mass destructive," or "mass casualty" consequences.
- The organization of the Federal Government's programs for combating terrorism is fragmented, uncoordinated, and politically unaccountable.
- Congress shares responsibility for the inadequate coordination of programs to combat terrorism.
- Insufficient attention has been paid to state and Federal capabilities.

Another national commission, the U.S. Commission on National Security/21st Century – the Rudman-Hart Commission – released its Phase III finding on January 31, 2001, with the following conclusions:[34]

- "The combination of unconventional weapons proliferation with the persistence of international terrorism will end the relative invulnerability of the U.S. homeland to catastrophic attack. A direct attack against American citizens on American soil is likely over the next quarter century."
- A new National Homeland Security Agency is needed to consolidate and refine the missions of the nearly two dozen disparate departments and agencies that have a role in U.S. homeland security.
- "Organizational reform is not a panacea...Sound organization is important. It can ensure that problems reach their proper level of decision quickly and efficiently."

With the changing cyber infrastructure, the conventional Federal control and regulatory policies are no longer adequate. In today's interdependent networks, a minor disruption means that system elements will not work properly. The Federal Government alone cannot ensure cyber security. Partnership with the private sector, based on a system of shared information and security intelligence is needed. As one telecommunications industry analyst has put it, the new policy question is not whether the government should get involved, but rather how.[35]

The partnership approach to addressing the cyber infrastructure risks involves a new policy perspective. As Dr. Rice has put it: "What we are talking about is a collaborative partnership between the public and private sectors that is unprecedented in our history. IT is a unique problem, and it's going to require unique solutions." These solutions should be formulated within the framework of a national risk communication strategy that addresses the full range issues relating to the shared public-private infrastructure. Loss of privacy, for instance, is a major issue to be addressed when the tradeoffs of privacy and security are evaluated.[36] Cyber policy issues such as the R&D funding priorities, training needs, and the potential anti-trust challenges arising from sharing intelligence and proprietary data also need to be addressed.

DOT must develop and coordinate specific methodologies, including a risk matrix, to secure IT infrastructure critical assets.

Security goals will be achieved by specifying goals and objectives, methodologies for achieving them, and criteria for evaluating performance. The DOT Office of Inspector General's audit on compliance with information security requirements concluded that DOT may not be able to secure its infrastructure critical assets by May 2003, as required by PDD-63, because DOT did not use any specific methodology; e.g., Project Matrix, recommended by the Critical Infrastructure Assurance Office (CIAO) to ensure comprehensive reviews of system dependencies, when identifying critical assets.

Deployment and transfer of technologies such as Project Matrix are critical to a risk communication plan. Project Matrix involves a 3-step process in which the Matrix team:

- Identifies and prioritizes each Federal agency's relevant assets.
- Provides a business process topology and identifies significant points of failure associated with critical assets.
- Identifies infrastructure dependencies associated with select assets.

Currently, 14 Federal agencies are voluntarily participating in Project Matrix. Preliminary reviews of 3 agencies, Social Security, Health and Human Services, and Treasury, determined that the 3 agencies collectively rely on roughly 4,000 physical and cyber assets to conduct day-to-day business. John Tritak, the CIAO Director, pointed out that Project Matrix provides a near-term risk management, as well as identifying nodes and networks that require robust cyber and physical vulnerability assessment. As a result of step one, the Matrix team determined that about 50 of the 4,000 assets required near-term priority attention.[37] With the help of such a matrix, priorities and risks can be addressed and potential threats mitigated.

Develop technologies and utilize existing tools to mitigate risk and ensure confidentiality, integrity, and availability.

As options for risk mitigation, countermeasures should be evaluated and prioritized with respect to system goals and requirements. Appendix B describes a number of security threat mitigation tools used to control access and ensure data integrity and network content security.

Access control is essential for ensuring confidentiality, integrity, and availability. It is designed to make sure that authorized people are able to do what they are authorized to do and everyone else is not. Access control has overlapping attributes with content privacy, dealing with confidentiality, integrity, and service availability threats. To control access, network security tools such as passwords, firewalls, intrusion detection devices, and value added networks are available.

For ensuring data integrity and content security on the Internet-based networks, many of the measures currently applied are not appropriate. Defending against network attacks is not as simple as incorporating cryptography into the system. Because domain naming system records constantly change, it is impractical to use digital signature or cryptographic authentication. Similarly, if all packets are encrypted, network engineers can no longer perform traffic analysis or use performance optimization systems.

Tools available for ensuring data integrity and network content security include cryptographic and non-cryptographic measures. Cryptographic tools include public key infrastructure, while non-cryptographic security measures include personal identification numbers, passwords, and biometrics. Tools such as Echelon and InfraGard are used at international or cross-agency levels as collaborative governmental initiatives to ensure cyber security.

In light of the new agencies formed to combat terrorism and protect critical infrastructure, state and local governments must work in tandem with the Federal Government to determine new roles and accountability.

The GAO report of September 2001 emphasized the need for more coordination. Other GAO congressional testimonies, dating as far back as October 6, 1999, have pointed out longstanding computer security weaknesses that place Federal operators at serious risk, including "the need for defining key agency roles and responsibilities" and evaluating "performance and oversight." The GAO testimony