

# OPINION SURVEY OF INFRASTRUCTURE OWNERS AND USERS

Report to the  
President's Commission  
on Critical Infrastructure Protection  
1997



This report was prepared for the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. The report represents the opinions and conclusions solely of its developer, Fleishman-Hillard, Inc.

# Table of Contents

---

<b>TABLE OF CONTENTS</b>	<b>II</b>
<b>EXECUTIVE SUMMARY</b>	<b>IV</b>
<b>Survey on infrastructure</b>	<b>iv</b>
<b>Survey of infrastructure owners</b>	<b>iv</b>
<b>Survey of infrastructure users</b>	<b>v</b>
<b>Comparisons of infrastructure owners and users</b>	<b>vii</b>
<b>INTRODUCTION</b>	<b>1</b>
<b>METHODS</b>	<b>3</b>
<b>DISCUSSION: INFRASTRUCTURE OWNERS</b>	<b>10</b>
<b>Perceptions of vulnerability</b>	<b>10</b>
<b>Perceptions of confidence of customers in the infrastructure</b>	<b>15</b>
<b>Elasticity: perceptions of the impact of events and practices on confidence in infrastructures</b>	<b>17</b>
<b>Initiatives to reduce infrastructure vulnerabilities</b>	<b>25</b>
<b>What are major issues affecting public confidence in infrastructures?</b>	<b>36</b>
<b>What kinds of events have damaged public confidence in infrastructures?</b>	<b>42</b>
<b>What actions do infrastructure owners take to reinforce public confidence?</b>	<b>44</b>
<b>DISCUSSION: INFRASTRUCTURE USERS</b>	<b>48</b>
<b>User perceptions the most critical infrastructure to company operations</b>	<b>48</b>
<b>User confidence in critical infrastructures</b>	<b>50</b>
<b>User perceptions of the vulnerabilities of infrastructures</b>	<b>52</b>
<b>What would be the effects of an infrastructure failure?</b>	<b>59</b>
<b>Major concerns about infrastructure failures</b>	<b>66</b>
<b>How have infrastructure failures affected companies</b>	<b>67</b>
<b>Elasticity: perceptions of the impact of events and practices on confidence in infrastructures</b>	<b>69</b>
<b>Systems used to protect operations from infrastructure failures</b>	<b>79</b>
<b>Perceptions of the transparency of infrastructure owners about reliability</b>	<b>83</b>



# Presidential Commission on Critical Infrastructure Protection

## Executive Summary

---

### Survey on infrastructure

**Methodology and timing of survey.** A total of 49 senior executives or senior managers with operational responsibilities within owners of key infrastructures were interviewed, as were 46 executives representing users of critical infrastructures. The interviews were conducted between July 21 and September 30, 1997.

### Survey of infrastructure owners

**Perceived infrastructure vulnerability.** Overall, executives do not feel that their infrastructures are very vulnerable to any of the threats, with half to two thirds rating their infrastructure as “not vulnerable.” The one exception is vulnerability to terrorism, with 30% of executives rating their infrastructure as very to extremely vulnerable. The infrastructures that feel more vulnerable have widely distributed facilities and/or highly visible facilities with public access.

**Perceptions of customer confidence in the infrastructures.** Infrastructure owners feel that their customers (business and consumer) have a high level of confidence in the ability of the infrastructure owner to provide continuous, reliable service.

**Elasticity of events on public confidence.** Company practices, procedures and operational reliability have the strongest positive impact in increasing public confidence in the company and the infrastructure. Transparency of company operations, proven reliability, and adherence to an external audit or standards are felt by executives to strongly increase public confidence in their infrastructures.

Conversely, executives feel that a lack of transparency, failure to meet standards and regulations, lack of preparation for operational failures or emergencies, and operational failures are the most significant factors that would decrease public confidence in their infrastructures.

**Initiatives to provide infrastructure protection.** Infrastructure owners implement a range of programs to prevent or minimize the vulnerability of their infrastructure to physical damage due to natural events, terrorism, cyber-terrorism, or employees, and to minimize the extent of damage should a terrorist or cyber-terrorist strike. The initiatives most commonly include hardened buildings and operating facilities, employee training, security systems, limited access to vulnerable and critical

systems, computer security systems, systems designed for early internal problem detection, redundant and backup systems, and contingency/emergency recovery planning.

***Major issues affecting public confidence in infrastructures.*** Infrastructure owners see that the major issues affecting public confidence are terrorism, operational problems that interrupt service, data security and privacy, the impact of deregulation, environmental issues, and confidence in the financial markets.

Specifically, infrastructure owners feel that three categories of events have actually reduced public confidence in their infrastructure: short-term interruptions of service, specific accidents and emergencies, and occurrences of possible fraud and deception that violated consumer trust.

***Initiatives to reinforce public confidence.*** Infrastructure owners recognize that they can reinforce public confidence in their infrastructures through public communications and education, providing reliable service, rapid communication of problems, and rapid restoration of service. They are taking the following steps to build public confidence:

- Build up a reserve of confidence and good will by transparency of company operations and communication with customers and with the community
- Design and operate highly reliable systems, and inform customers and the community about the system
- Quickly and honestly inform customers and the community about service interruptions, outages, or accidents when they occur
- Rapidly restore service after a service interruption

## **Survey of infrastructure users**

***Most critical infrastructures to company operations.*** Business executives resoundingly feel that telecommunications and electric power are the most critical infrastructures to their company operations, followed by banking & finance and transportation. Oil and natural gas are a relatively distant fifth.

***User confidence in critical infrastructures.*** Overall, the business executives surveyed are quite confident that the critical infrastructures are and will be able to provide reliable, dependable services that are essential to their own operations. Infrastructure users are most confident in the banking & financial systems and in the telecommunications infrastructure. Users are somewhat less confident in the energy production, transportation and distribution systems (electric, oil and natural gas).

Users less confident, but only relatively less so, in the transportation systems, including airlines, railroads, trucking, shipping and public transportation. The lengthy United Parcel Service strike, which covered much of the interviewing period, may have influenced perceptions of vulnerability to disruption of transportation systems.

***User perceptions of infrastructure vulnerabilities.*** Business users do not feel that critical infrastructures are particularly vulnerable to disruption by technical failures, human error, terrorism, cyber-terrorism or disgruntled employees, although their verbatim comments indicate that they are certainly aware of potential threats.

The telecommunications and electric power infrastructures are seen as the most vulnerable across all types of threats. Disruption by disgruntled employees or other insiders is seen as the largest threat to all infrastructures. For the energy infrastructures, terrorism is seen as the second largest threat. For the telecommunications, banking and financial infrastructures, cyber-terrorism is seen as the second most important threat.

### ***Impact of an infrastructure failure***

***Electric power.*** Failure of the electric power infrastructure has an impact on businesses in a time frame that ranges from immediate shut-down to companies that can operate for a few hours or those that can operate for a few days. Fewer than about one fifth have backup systems that permit continuous operation through an interruption of electric power.

***Natural gas and oil.*** Direct dependence on natural gas and oil appears to be less critical to most companies. While a number feel that disruption of natural gas or oil supplies would slow down operations, almost none feel that the disruption would *stop operations*.

***Telecommunications.*** All respondents felt that a failure or major disruption of telecommunications would have a significant impact on business operations. However, companies were nearly evenly divided on their assessment as to whether a crisis would develop in less than 24 hours or if they could continue for a longer period of time. Fewer than one fifth reported that they have backup systems that would compensate for a telecommunications failure. Virtually all other companies indicated that a telecommunications failure would have significant impact on operations.

***Banking and financial services.*** Very few companies felt that a disruption of banking and financial services would adversely affect operations in the short term. A system failure would affect operations starting between two days and two weeks. The major issues noted across all industries participating in the survey centered around three themes: the inability to access funds or loans, the impossibility of

conducting a variety of transactions, and a halt in their ability to efficiently conduct transactions.

*Transportation.* The impact of a disruption of transportation varied by industry. Companies feeling a disruption in transportation would affect them quickly (two days or less) tended to be manufacturers and consumer products companies. Most respondents felt they could operate on a longer term without various modes of transportation. Several service-oriented companies not involved in the delivery of the product noted that a disruption of transportation infrastructures would not directly affect their operations.

### ***Elasticity of impact of events on user confidence in infrastructures.***

Infrastructure users feel that company practices, procedures and operational reliability have the strongest positive impact on their confidence in infrastructures. Note that these are the same forces that infrastructure owners feel tend to increase public confidence.

- ***Contingency or emergency planning and preparation*** lead all other actions in increasing business confidence in infrastructures including, it is interesting to note, proven reliability. Regular rehearsal of a backup plan and presence of backup systems are the two leading factors that increase confidence.
- ***Proven reliability*** in providing services also stands out as an extremely strong factor enhancing confidence. We can speculate that proven reliability is a cost-of-entry for an infrastructure provider, but that the ability to handle crises and system failures differentiates among infrastructure owners.

For business users, knowledge that an infrastructure computer system can resist a computer hacker also strongly increases confidence. For infrastructure owners, this type of event received more mixed ratings.

- ***Transparency*** of company operations and planning is viewed as critical. The companies feel that infrastructure owners should inform business customers about their operations.

Correspondingly, infrastructure users feel that a lack of recovery planning, lack of transparency, failure to meet standards and regulations, and operational failures are the most significant factors that would decrease their confidence.

## **Comparisons of infrastructure owners and users**

In general, infrastructure owners and infrastructure users have similar attitudes to infrastructure dependability and reliability.

- Both groups feel that the critical infrastructures are dependable and reliable.

- Infrastructure owners are more likely to be concerned about physical damage due to terrorism than are users.
- Owners and users have nearly identical perceptions of the “elasticity” of the impact of events on confidence in the infrastructure. This suggests that owners understand key issues that impact user confidence, and presumably will take steps necessary to maintain user confidence.

Owner and user perspectives differ in one area. Infrastructure users are more concerned about periodic service outages even though service is restored rapidly than are infrastructure owners. It can be inferred that owners have technical confidence in the ability of their infrastructures to meet customer needs. Infrastructure users view technical reliability as a cost-of-entry for infrastructure owners, and assume a high level of dependability and reliability. However, infrastructure users appear to be concerned about the possibility of infrastructure failures, which entail real costs for the user. Users may be less forgiving of periodic outages or disruptions than owners assume them to be.

# Presidential Commission on Critical Infrastructure Protection

## Survey of Infrastructure Owners and Business Users

### Introduction

---

The President's Commission on Critical Infrastructure Protection was established to recommend a policy and an implementation strategy for protecting critical U.S. infrastructures against both physical and cyber threats, and assuring their continued operations. Critical infrastructures are defined as those systems and services so vital that their incapacity or destruction would have a debilitating impact on the defense or economic competitiveness of the United States. These infrastructures represent national "life support systems" and include information and communications, energy, transportation, banking and finance, and vital human services.

In order to assist in gaining an understanding of the drivers of public confidence in critical infrastructures, the Commission has conducted a number of outreach initiatives including meetings and public hearings. The Commission asked Fleishman-Hillard Research to undertake two surveys. The first survey was conducted with senior executives at ***companies that own and operate critical infrastructures***, such as telecommunications companies, energy utilities, Internet service providers, banks, financial institutions, and transportation companies. The objectives of the survey were to understand how infrastructure owners view the ability of critical infrastructures to withstand physical and cyber threats, what the infrastructure owners and operators are doing to protect the operations, and what these owners are doing to generate public confidence in their ability to provide continuous, reliable services.

The second survey was conducted with senior executives at ***companies that use and rely upon critical infrastructures***. The objectives of the survey were to understand how confident infrastructure users are in the ability of critical infrastructures to withstand physical and cyber threats, what would be the effects of an infrastructure failure, and what the infrastructure users are doing to protect their own operations from infrastructure failures. This report, which summarizes the results of the survey research, is organized in the following sequence:

- Methods
- Analysis and discussion of the "owners" research

- Analysis and discussion of the “users” research
- Comparisons of viewpoints of owners and users on reliability of critical infrastructures
- Survey questionnaires (Appendix)

## Methods

---

### ***Questionnaire***

The Fleishman-Hillard project team developed two survey instruments, one for the infrastructure owners and one for the infrastructure users, working in close collaboration with the PCCIP project director (see Appendix). The questionnaires were designed to provide a mix of closed-ended questions and open-ended questions, in order to allow survey participants to elaborate upon topics of particular importance to their company or infrastructure. The questionnaires were tested in a series of actual interviews with business executives, and then revised based on the test results.

### ***Interview procedures***

The Fleishman-Hillard Research executive interviewing staff conducted interviews with a total of 49 senior executives or senior managers with operational responsibilities at owners of key infrastructures, and 46 interviews with executives at users of critical infrastructures, between July 21 and September 30, 1997. All interviews were conducted from Fleishman-Hillard Research interviewing facilities in St. Louis. Most interviews lasted between 15 and 25 minutes, with a few slightly longer or shorter. Most infrastructure users were unfamiliar with the Commission, and requested additional information about the Commission before agreeing to complete the interview. A fact sheet on the Commission was sent by fax to potential participants. Most infrastructure owners already had some knowledge of the Commission.

### ***Infrastructures and survey participants***

#### **• Infrastructure owners**

Fleishman-Hillard Research developed a list of companies in the target infrastructures, working in consultation with the PCCIP project team. Particular attention was placed on completing interviews with the following key infrastructures (see Figure 1):

- Telecommunications systems (local, long distance and cellular)
- Financial networks that depend upon computer networks and telecommunications (ATM networks, bank clearing networks, financial markets and banks)
- Energy generation, transmission and distribution (electricity, natural gas and oil)
- Transportation (airlines, trucking, railroads, public transit, overnight delivery)

The Fleishman-Hillard interviewing team then identified qualified respondents. Qualified respondents were either members of the senior management team, or had senior operational responsibilities within the organization (See Figure 2).

**Figure 1: Number of completed interviews by infrastructure**

<b>Infrastructure</b>	<b>Completed interviews</b>
<b>Computers &amp; Telecommunications (total)</b>	<b>16</b>
<i>Internet Service Provider</i>	5
<i>Cellular Telephone</i>	4
<i>Local Telephone</i>	4
<i>Cable TV</i>	2
<i>Long Distance Telephone</i>	1
<b>Transportation (total)</b>	<b>16</b>
<i>Public Transportation</i>	7
<i>Airports</i>	3
<i>Overnight Delivery</i>	2
<i>Railroads</i>	2
<i>Airlines</i>	1
<i>Trucking</i>	1
<b>Banking &amp; financial services (total)</b>	<b>7</b>
<i>Banking-ATM Networks</i>	2
<i>Banking-Clearing Systems</i>	2
<i>Financial Markets</i>	2
<i>Banks-National</i>	1
<b>Energy production, transmission &amp; distribution (total)</b>	<b>7</b>
<i>Electric Utilities</i>	3
<i>Natural Gas</i>	2
<i>Oil Companies</i>	2
<b>Other infrastructures (total)</b>	<b>3</b>
Emergency Services	2
Other	1
<b>Total</b>	<b>49</b>

**Figure 2: Job titles of survey respondents by industry**

<b>Industry</b>	<b>Job title</b>
Airline	CEO/COO
Airport	Executive Director
Airport	Airport Manager
Airport	Chief of Airport Police
Banking-ATM Network	VP Computer Operations
Banking-ATM Network	Senior Vice President
Banking-Clearing System	VP Computer Operations
Banking-Clearing System	Director of Automation Services
Bank-National	Recovery Coordinator
Bank-Regional	Security Manager
Cable TV	VP Information Systems
Cable TV	CEO/COO
Cellular Telephone	VP Information Systems
Cellular Telephone	VP Corporate Security
Cellular Telephone	VP Information Systems
Cellular Telephone	Director of Networks
Electric Utility	Operations Manager
Electric Utility	VP Planning/Operations
Electric Utility	VP Management Services and Telecommunications
Emergency Services	CEO/COO
Emergency Services	Commissioner
Financial Market	VP Information Systems
Financial Market	CEO/COO
Internet Service Provider	Security Manager
Internet Service Provider	President
Internet Service Provider	VP Planning/Operations
Internet Service Provider	VP Planning/Operations
Internet Service Provider	CIO
Natural Gas	VP Corporate Security
Natural Gas	President

<b>Industry</b>	<b>Job title</b>
Oil Company	Security Manager
Oil Company	Security Manager
Overnight Delivery	Senior Manager - Enterprise Data
Overnight Delivery	VP Public Affairs
Public Transportation	Manager: Business Development
Public Transportation	Commissioner
Public Transportation	Manager: Communications
Public Transportation	Deputy General Manager
Public Transportation	VP Information Systems
Public Transportation	General Manager
Public Transportation	Deputy General Manager
Railroads	Refused
Railroads	VP Planning/Operations
Local Telephone	VP Planning/Operations
Local Telephone	Chief Technology Officer
Local Telephone	VP/GM Industry
Local Telephone	Executive VP Communication and Information Products
Long Distance Telephone	CEO/COO
Trucking	President

- **Infrastructure users**

Fleishman-Hillard Research worked in consultation with the PCCIP project team to develop a list of target companies that are users of critical infrastructures. Figure 3 lists the number of completed interviews by business category.

**Figure 3: Number of completed interviews by infrastructure**

<b>Business sector</b>	<b>Interviews</b>
Banking	4
Consumer products	6
Direct marketing	2
Financial services	2
Healthcare	3
Insurance	4
Manufacturing	7
Pharmaceuticals	2
Publishing/ broadcast	2
Restaurants/ hotels	2
Retail	4
Technology	7
Telecommunications	1
	<b>46</b>

The Fleishman-Hillard interviewing team then identified qualified respondents who would understand the company’s vulnerabilities to disruption or failure of critical infrastructures. Qualified respondents were either members of the senior management team, or had senior operational responsibilities within the organization (See Figure 4).

**Figure 4: Job titles of survey respondents by industry (users)**

<b>Industry</b>	<b>Job title</b>
Banking-national	VP & Manager of Contingency Management
Banking-national	VP Computer Operations
Banking-regional	Director of Corporate Security
Banking-regional	Security Manager
Consumer products	Director of Corporate Security
Consumer products	MIS Director

<b>Industry</b>	<b>Job title</b>
Consumer products	Director of Internal Audits
Consumer products	Sr. Technology Manager & Corp. Security
Consumer products	VP Information Systems
Consumer products	VP Information Systems
Direct marketing	VP Tech Infrastructure
Direct marketing	VP Information Systems
Financial services	Director of Business Continuation/Business Continuation Consultant
Financial services	Security Manager
Health care	MIS Director
Health care	MIS Director
Health care	Facility Manager
Insurance	Chief Technology Officer
Insurance	VP
Insurance	VP Information Systems
Manufacturing	CEO/COO/CFO
Manufacturing	Director of Telecommunications
Manufacturing	Director of Government Affairs
Manufacturing	Information Services Manager
Manufacturing	Infrastructure Manager
Manufacturing	Chief Architect-Info Tech.
Manufacturing	VP Information Systems
Pharmaceuticals	VP Corp. Security
Pharmaceuticals	VP Corporate Development
Publishing/ broadcast	VP Computer Operations
Publishing/ broadcast	Security Manager
Restaurants/ hotels	Government Relations Rep.
Restaurants/ hotels	VP Risk Management
Retail	MIS Director
Retail	Corp. VP Employee Relations
Retail	VP Information Systems

---

<b>Industry</b>	<b>Job title</b>
Retail	VP Information Systems
Technology	Director of Engineering Services
Technology	Information Security
Technology	Senior Manager Info Protection
Technology	VP & General Counsel
Technology	VP Enterprise Networks
Technology	Security Supervisor
Technology	Internet Service Provider
Telecommunications	Director of Network Security

## Discussion: Infrastructure Owners

---

### Perceptions of vulnerability

Survey participants were asked to rate the vulnerability of their company's infrastructure to four kinds of threat:

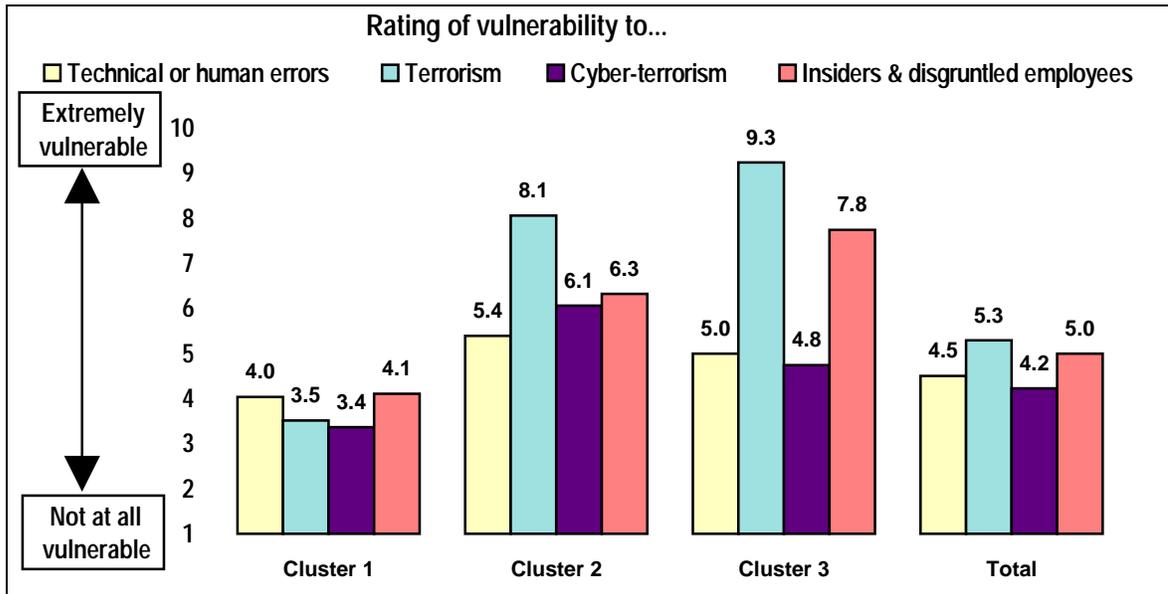
- technical failures and human error
- physical damage due to terrorism
- disruption of telecommunications and computer networks due to cyber-terrorism
- disruption of telecommunications and computer networks by insiders or disgruntled employees

Overall, executives do not feel that their infrastructures are very vulnerable to any of the threats, with half to two thirds rating their infrastructure as “not vulnerable.” The one exception is vulnerability to terrorism, with 30% of executives rating their infrastructure as 8, 9 or 10 on a 10-point scale where 10 means “extremely vulnerable” (Figure 5, Figure 6 & Figure 7).

### ***Vulnerability to technical problems and human errors***

- Two thirds (67%) rate their vulnerability between 1 and 5 on a 10 point scale where 1 means “Not at all vulnerable” and 10 means “Extremely vulnerable” (average rating = 4.5).
- Only about 12% rate their vulnerability as relatively high, with ratings of 8, 9 or 10 on the 10 point scale.
- The companies that consider themselves to be particularly vulnerable (rating 8, 9 or 10 on the 10-point scale) include public transit, and a mix of other several other infrastructures.

**Figure 5: Perceived vulnerabilities to threats**



**Figure 6: Perceived vulnerabilities to threats**

Corner	Mean	Standard Error of Mean	Standard Deviation	Valid N
Vulnerable to technical errors or human errors	4.51	.32	2.23	N=47
Vulnerable to physical damage due to terrorists	5.30	.43	2.95	N=47
Vulnerable to disruption of computer/telecommunications due to cyber terrorism	4.23	.34	2.34	N=48
Vulnerable to disgruntled employees	5.00	.35	2.41	N=48

10 point rating scale where 1 = "Not at all vulnerable" and 10 = "Extremely vulnerable"

**Figure 7: Perceived vulnerabilities to threats**

	Vulnerable to technical errors or human errors		Vulnerable to physical damage due to terrorists		Vulnerable to disruption of computer/telecommunications due to cyber terrorism		Vulnerable to disgruntled employees	
	Count	%	Count	%	Count	%	Count	%
Not at all vulnerable	1	2.0%	4	8.2%	4	8.2%	2	4.1%
2	8	16.3%	8	16.3%	10	20.4%	7	14.3%
3	11	22.4%	6	12.2%	9	18.4%	7	14.3%
4	6	12.2%	2	4.1%	5	10.2%	4	8.2%
5	7	14.3%	4	8.2%	6	12.2%	8	16.3%
6	5	10.2%	4	8.2%	4	8.2%	7	14.3%
7	3	6.1%	5	10.2%	4	8.2%	5	10.2%
8	3	6.1%	6	12.2%	5	10.2%	4	8.2%
9	2	4.1%	4	8.2%	0	.0%	2	4.1%
Extremely vulnerable	1	2.0%	4	8.2%	1	2.0%	2	4.1%
Don't know	2	4.1%	2	4.1%	1	2.0%	1	2.0%
Total	49	100.0%	49	100.0%	49	100.0%	49	100.0%

10 point rating scale where 1 means "Not at all vulnerable" and 10 means "Extremely vulnerable"

***Vulnerability to terrorism***

Most companies do not consider themselves especially vulnerable to physical damage due to terrorism. The exceptions are companies with distributed facilities and public access.

- Just under half (49%) rate their company’s vulnerability between 1 and 5 on the 10 point scale (average rating = 5.3).
- However, 29% rate their vulnerability as relatively high, with ratings of 8, 9 or 10 on a 10 point scale (10 = “Extremely vulnerable”).
- The industries that consider themselves to be particularly vulnerable to terrorism fall into two general categories:
  - Companies with distributed facilities (e.g., natural gas, electric utilities, railroads and overnight delivery)
  - Companies with highly visible facilities that also offer public access (airports, public transit, banks and emergency services)

### ***Vulnerability to cyber-terrorism***

Most companies feel that they are not particularly vulnerable to disruption of computer systems of telecommunications due to cyber-terrorism.

- About two thirds (69%) rate their vulnerability between 1 and 5 on a 10 point scale where 1 means “Not at all vulnerable” and 10 means “Extremely vulnerable” (average rating = 4.2).
- Just over one tenth (12%) rate their vulnerability as relatively high, with ratings of 8, 9 or 10 on the 10 point scale.
- Relatively few infrastructure owners that consider themselves to be vulnerable to cyber-terrorism—an airline, two airports, one public transit system, one emergency services system, and one railroad.

### ***Vulnerability to disruption of computer and telecommunications systems due to insiders and disgruntled employees***

Companies feel that they are not very vulnerable to the disruption of computer and telecommunications by disgruntled employees or insiders with access to these systems.

- Somewhat over half (57%) rate their vulnerability between 1 and 5 on a 10 point scale where 1 means “Not at all vulnerable” and 10 means “Extremely vulnerable” (average rating = 5.0).
- Under one fifth (16%) rate their vulnerability as relatively high, with ratings of 8, 9 or 10 on the 10 point scale.
- There is no particular pattern to the infrastructure owners that consider themselves especially vulnerable to the disruption of telecommunications or computer systems by insiders or disgruntled employees. The infrastructures that are most closely involved in telecommunications and computer networks (e.g., banks and related financial infrastructures; Internet service providers; and cellular, local and long distance telephone companies) consider themselves to be least vulnerable to insiders and disgruntled employees.

### ***Perceptions of vulnerability by industry***

The companies can be divided into three groups based on their perceived vulnerabilities. This grouping is based on a single-link hierarchical cluster analysis using the four “vulnerability” variables discussed in this section (Figure 5).

- Companies in cluster 1 have ***low perceived vulnerabilities to all threats***. It is interesting to note that this cluster includes most of the companies that either provide computer networking or telecommunications networking services (telephone companies and Internet service providers), and companies that

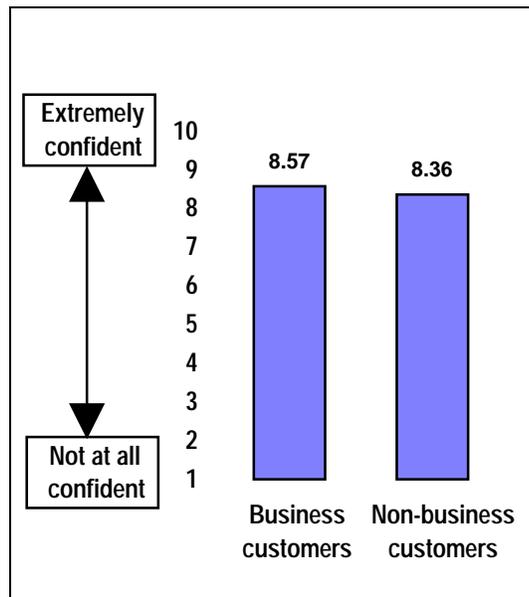
are entirely dependent upon computer networking and telecommunications in order to perform their basic services. This cluster includes the following types of companies in particular:

- All ATM networks (n=2) and one of the two bank clearing systems
- All financial markets (n=2)
- All local and long distance telephone companies (n=3), and three of four cellular telephone companies.
- Most electric utilities (two of three)
- All Internet service providers (n=5)
- A mixture of oil companies, natural gas companies, railroads, trucking companies, public transit systems, airlines and airports
- Companies in cluster 2 have ***higher perceived vulnerabilities to terrorism*** than cluster 1, and the ***highest perceived vulnerabilities to technical & human errors, and to cyber-terrorism***. This cluster includes the following types of companies in particular:
  - Two of three airports
  - All emergency medical systems (n=2)
  - All overnight delivery systems (n=2)
  - Most of the public transit systems (four of six)
  - A mixture of natural gas companies, airlines, airports, cable television, cellular telephone, and bank clearing systems
- Companies in cluster 3 have the ***highest perceived vulnerabilities to both terrorism and to cyber-terrorism by insiders and disgruntled employees***. In this small sample, there is no particular pattern to the industries included within this category, which includes an oil company, a railroad, a national bank, a public transportation network and a cable television company.

## Perceptions of confidence of customers in the infrastructure

All infrastructure owners feel that their customers—both business customers and non-business customers—have a high level of confidence in the ability of the infrastructure owner to provide continuous, reliable service. Indeed, 88% feel that business customers are very to extremely confident in their infrastructure, and 80% feel that non-business customers are very to extremely confident (Figure 8, Figure 9 & Figure 10).<sup>1</sup>

**Figure 8: Perceptions of customer confidence in the infrastructure owner  
(Excludes “Don’t know” responses)**



**Figure 9: Perceptions of customer confidence in the infrastructure owner  
(Excludes “Don’t know” responses)**

	Mean	Standard Error of Mean	Standard Deviation	Valid N
Business customer confidence in ability to provide reliable service	8.57	.17	1.19	N=47
Non-business customer confidence in ability to provide reliable service	8.36	.25	1.43	N=33

Rating scale where 1 = "Not at all confident" and 10 = "Extremely confident"

<sup>1</sup> Ratings of 8, 9 or 10 on a 10-point scale where 10 means that they feel customers are “extremely confident.” The “don’t know” responses are excluded because these respondents tended to feel that they do not have sufficient contact with customers to make a judgment.

**Figure 10: Perceptions of customer confidence in the infrastructure owner**

	Business customer confidence in ability to provide reliable service		Non-business customer confidence in ability to provide reliable service	
	Count	%	Count	%
3	0	0%	1	2%
5	2	4%	0	0%
6	2	4%	2	4%
7	1	2%	3	6%
8	12	24%	8	16%
9	22	45%	14	29%
Extremely confident	8	16%	5	10%
Don't know	2	4%	16	33%
Total	49	100%	49	100%

10 point rating scale where 1 means "Not at all confident" and 10 means "Extremely confident"

## Elasticity: perceptions of the impact of events and practices on confidence in infrastructures

In order to estimate the impact that certain types of events would have on public confidence in an infrastructure, respondents were asked to indicate whether they felt that a certain set of events would strongly increase, slightly increase, neither increase nor decrease, slightly decrease or strongly decrease public confidence in the ability of their infrastructure to provide continuous, reliable, high-quality products and services.

### *Events that are perceived as increasing public confidence*

Executives feel that company practices, procedures and operational reliability have the strongest positive impact in increasing public confidence in the company and the infrastructure (Figure 11 & Figure 12; data in Figure 16 & Figure 17).

- **Transparency** of company operations and planning is viewed as critical. The companies feel that they should inform the community about their operations, their backup systems, and their emergency response plans.
- **Proven reliability** in providing services stands out as the strongest factor enhancing public confidence. Nearly three quarters of respondents (71%) feel that a record of five years of service without a major outage will “strongly increase” public confidence. This is by far the single highest rating of “strongly increase.”
- Adherence to an **external audit or standard** established by a legitimating authority, such as an industry code, can also be a powerful guarantee.

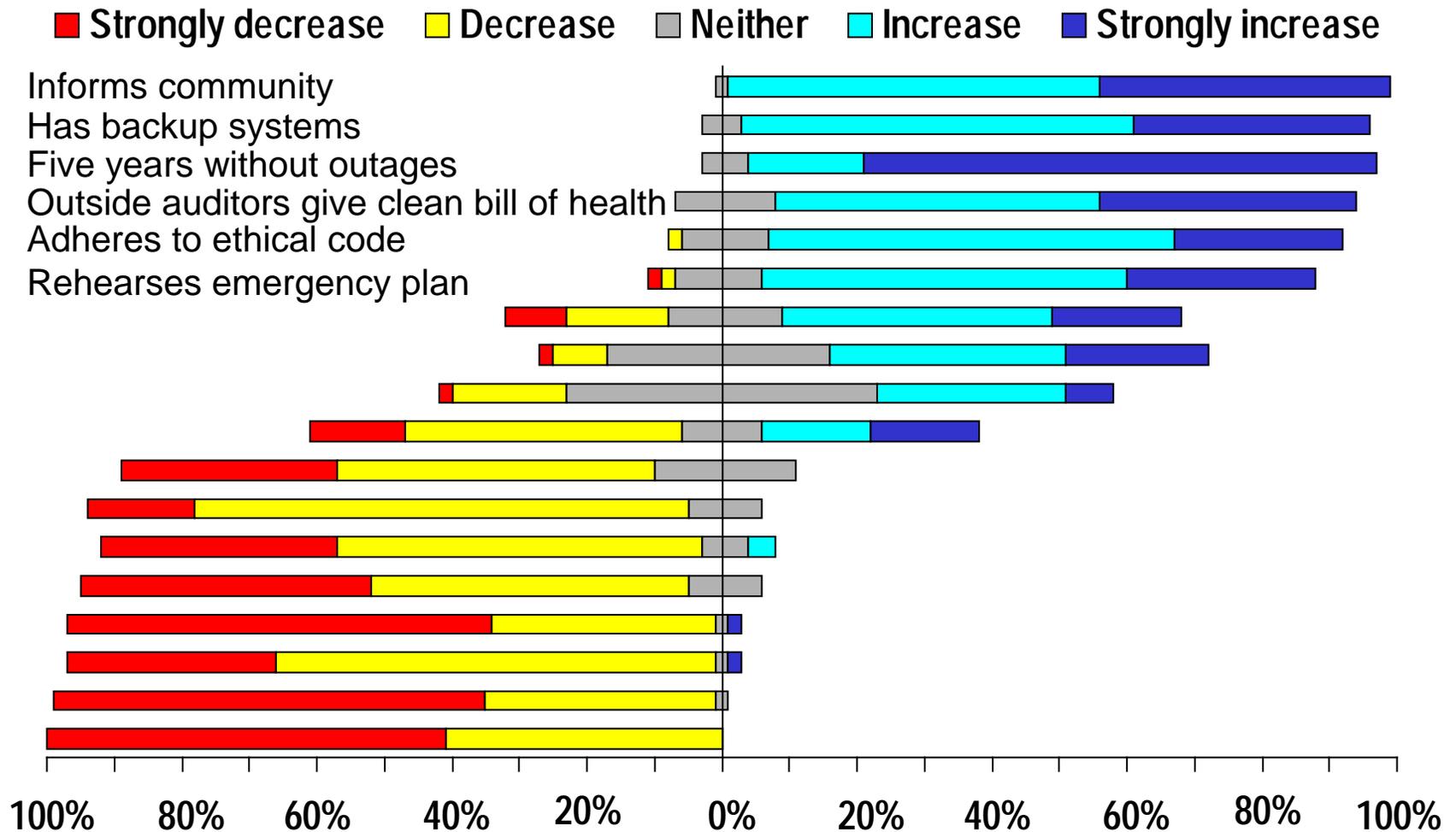
**Figure 11: Events that are felt to increase public confidence in infrastructures**  
(Excludes “Don’t know” responses)

The company...	“Strongly increase” or “slightly increase”
Informs the community about operations	98%
Has backup systems in place	94%
Reports no service outages in five years	93%
Outside auditors give company a clean bill of health	85%
Voluntary adherence to ethical code	85%
Rehearses emergency response plan	83%

***Figure 12: Events that are felt to increase public confidence in infrastructures***

**[Insert PowerPoint slide here]**

# Figure 12: What factors increase public confidence in infrastructures (Owners)?



### ***Events that are perceived as decreasing public confidence***

Corresponding to the results in the previous section, executives feel that a lack of transparency, failure to meet standards and regulations, lack of preparation for operational failures or emergencies, and operational failures are the most significant factors that would decrease public confidence in their respective infrastructures (Figure 13 & Figure 14; data in Figure 16 & Figure 17).

- ***Lack of transparency.*** Failure to inform the community about operations, and, most of all, deception strongly diminish public confidence.
- ***Failure to meet standards and regulations for operations,*** for example, when outside auditors find security or reliability problems, or the company is fined for violation of a regulation, are seen as decreasing public confidence.
- ***Lack of preparation for system failures,*** for example, if the company has no backup systems or has no emergency systems decrease public confidence.
- ***Operational failures,*** such as a successful entry into a computer system by a computer hacker, or a major outage caused by a computer system failure decrease confidence in the ability of an infrastructure to deliver services reliably and dependably.

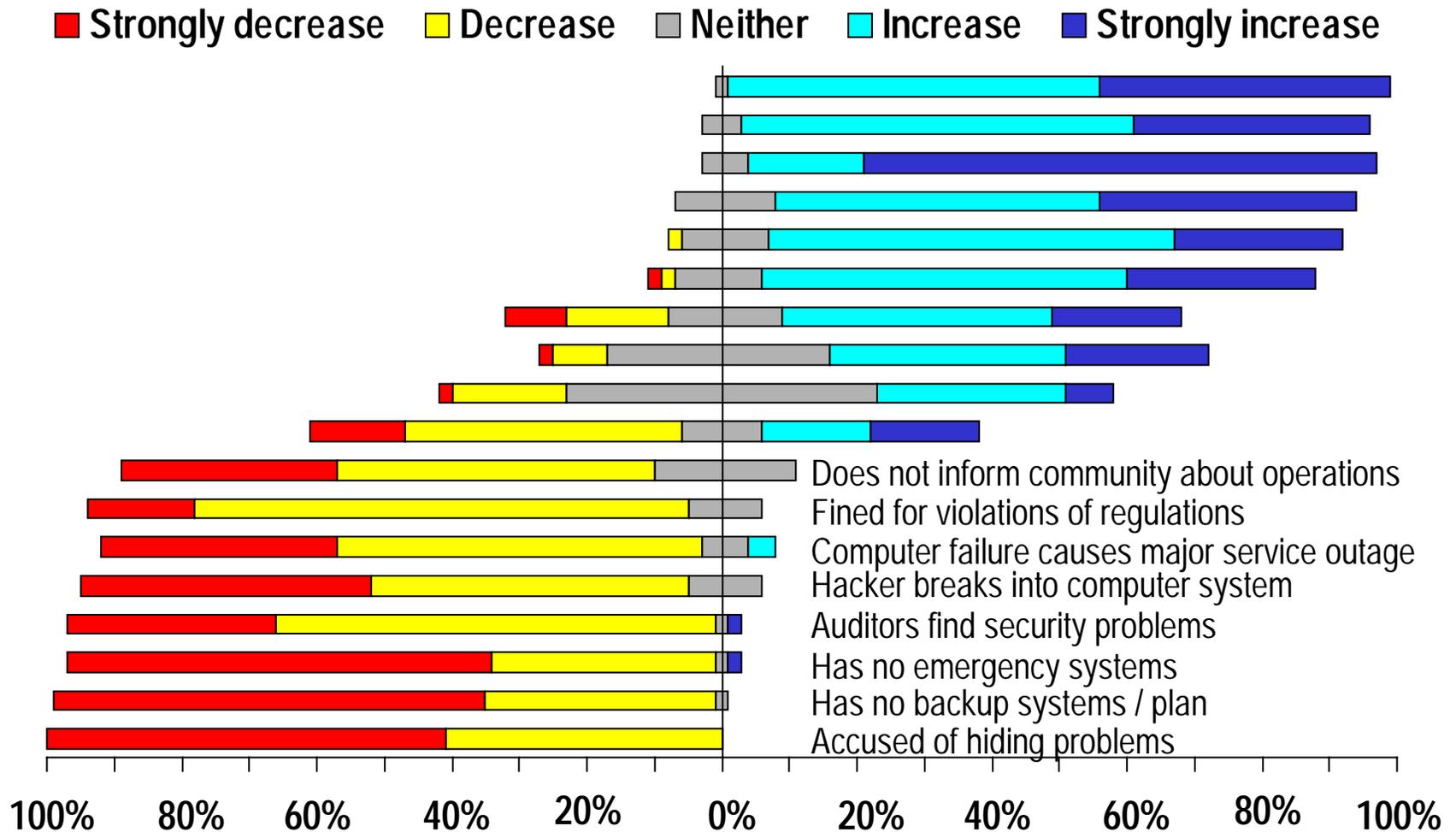
***Figure 13: Events that are felt to decrease public confidence in infrastructures  
(Excludes “Don’t know” responses)***

	“Strongly decrease” or “slightly decrease”
Company accused of hiding problems	100%
Company has no backup systems	98%
Company has no emergency systems	96%
Auditors find security/reliability problems	96%
Computer hacker successfully enters system	89%
Computer failure causes major outage	89%
Company fined for violations of regulations	89%
Company does not inform community	89%

***Figure 14: Events that are felt to decrease public confidence in infrastructures***

**[Insert PowerPoint slide here]**

# Figure 14: What factors decrease public confidence in infrastructures (Owners)?



### ***Events that are perceived as having mixed effects on confidence in infrastructures***

Four events have mixed effects on the confidence of business customers in infrastructures. These events have in common the fact that they involve the identification of infrastructure problems on the one hand, which would tend to decrease confidence, but also involve the elaboration of a plan to rectify those problems, which would have the effect of increasing confidence (Figure 15; data in Figure 16 & Figure 17).

Three events generally increase confidence, but decrease confidence for some:

- Company identifies problems and announces a plan to resolve those problems within one year
- Hacker unsuccessfully attempts to break into a computer system
- Government enforces minimum standards for reliability

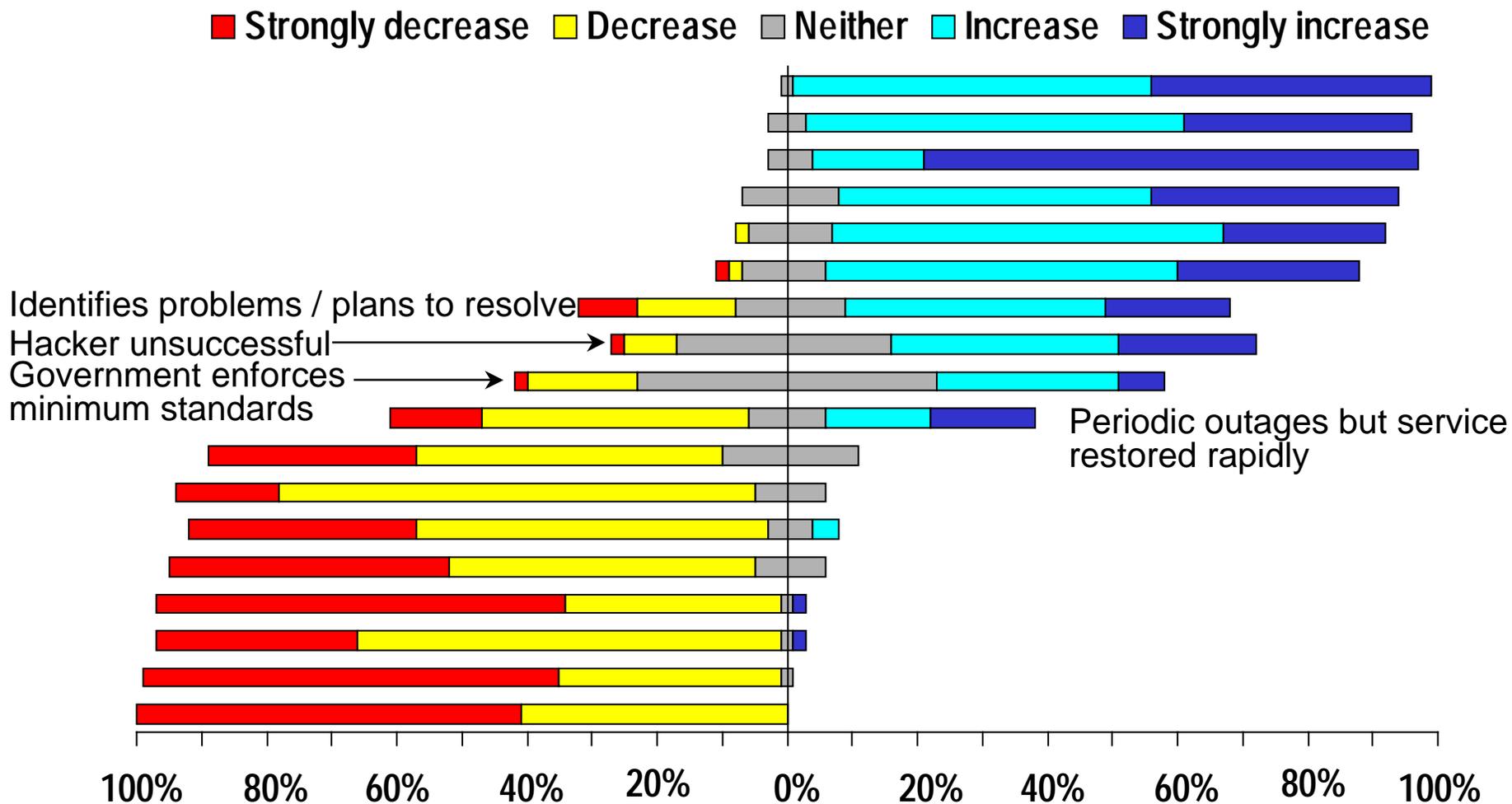
One situation is felt to generally decrease confidence, but increase confidence for some due to proven ability to recover from emergency situations:

- Company has a record of periodic service outages, but restores service rapidly

***Figure 15: Events that have mixed impact on public confidence in infrastructures***

[Insert Powerpoint slide]

# Figure 15: What factors have mixed effects on public confidence in infrastructures (Owners)?



**Figure 16: Impact of events on public confidence in infrastructures**

	Mean	Standard Error of Mean	Standard Deviation	Valid N
Company reports five years of service with no outages	4.70	.09	.59	N=46
Major service outage due to a computer problem	1.80	.11	.75	N=46
Record of periodic outage but restores services rapidly	2.80	.19	1.34	N=49
Hacker unsuccessful at entering computer system	3.65	.14	.98	N=48
Hacker successfully broke into computer system	1.68	.10	.66	N=47
Company is fined for violating a regulation	1.95	.08	.53	N=44
Voluntarily adheres to code for ethical business practices	4.08	.10	.68	N=48
Government enforces minimum standards for reliability	3.20	.13	.88	N=46
Has backup system in case of failures	4.29	.08	.58	N=48
Has no backup systems in case of failures	1.38	.08	.53	N=47
Has no adequate emergency response plan	1.46	.11	.75	N=46
Regularly rehearses its emergency response plan	4.04	.12	.84	N=46
Outside auditors give clean bill of health for security/ reliability	4.23	.10	.69	N=48
Outside auditors find security and reliability problems	1.77	.10	.69	N=48
Company keeps community informed about its operations	4.41	.08	.54	N=49
Company does not keep community informed about its operation	1.89	.11	.73	N=47
Company identifies problems and announces plan to resolve them within one year	3.47	.18	1.21	N=47
Company accused of hiding problems of security or reliability	1.41	.07	.50	N=49

Rating scale where 1 = "Strongly decrease confidence," 2 = Slightly decrease confidence," 3 = "Neither," 4 = "Slightly increase confidence" and 5 = "Strongly increase confidence"

**Figure 17: Impact of events on public confidence in infrastructures**

		Strongly decrease	Slightly decrease	Neither	Slightly increase	Strongly increase	Don't know/refused	Total
Company reports five years of service with no outages	Count	0	0	3	8	35	3	49
	%	0%	0%	6%	16%	71%	6%	100%
Major service outage due to a computer problem	Count	16	25	3	2	0	3	49
	%	33%	51%	6%	4%	0%	6%	100%
Record of periodic outage but restores services rapidly	Count	7	20	6	8	8	0	49
	%	14%	41%	12%	16%	16%	0%	100%
Hacker unsuccessful at entering computer system	Count	1	4	16	17	10	1	49
	%	2%	8%	33%	35%	20%	2%	100%
Hacker successfully broke into computer system	Count	20	22	5	0	0	2	49
	%	41%	45%	10%	0%	0%	4%	100%
Company is fined for violating a regulation	Count	7	32	5	0	0	5	49
	%	14%	65%	10%	0%	0%	10%	100%
Voluntarily adheres to code for ethical business practices	Count	0	1	6	29	12	1	49
	%	0%	2%	12%	59%	24%	2%	100%
Government enforces minimum standards for reliability	Count	1	8	21	13	3	3	49
	%	2%	16%	43%	27%	6%	6%	100%
Has backup system in case of failures	Count	0	0	3	28	17	1	49
	%	0%	0%	6%	57%	35%	2%	100%
Has no backup systems in case of failures	Count	30	16	1	0	0	2	49
	%	61%	33%	2%	0%	0%	4%	100%
Has no adequate emergency response plan	Count	29	15	1	0	1	3	49
	%	59%	31%	2%	0%	2%	6%	100%
Regularly rehearses its emergency response plan	Count	1	1	6	25	13	3	49
	%	2%	2%	12%	51%	27%	6%	100%
Outside auditors give clean bill of health for security/ reliability	Count	0	0	7	23	18	1	49
	%	0%	0%	14%	47%	37%	2%	100%
Outside auditors find security and reliability problems	Count	15	31	1	0	1	1	49
	%	31%	63%	2%	0%	2%	2%	100%
Company keeps community informed about its operations	Count	0	0	1	27	21	0	49
	%	0%	0%	2%	55%	43%	0%	100%
Company does not keep community informed about its operations	Count	15	22	10	0	0	2	49
	%	31%	45%	20%	0%	0%	4%	100%
Company identifies problems and announces plan to resolve them within one year	Count	4	7	8	19	9	2	49
	%	8%	14%	16%	39%	18%	4%	100%
Company accused of hiding problems of security or reliability	Count	29	20	0	0	0	0	49
	%	59%	41%	0%	0%	0%	0%	100%

Rating scale where 1 means "Strongly decrease," 2 means "Slightly decrease," 3 means "Neither," 4 means "Slightly increase" and 5 means "Strongly increase"

## **Initiatives to reduce infrastructure vulnerabilities**

Infrastructure owners were asked to describe the steps they are taking to reduce their vulnerability to four types of threats:

- technical failures and human error
- physical damage due to terrorism
- disruption of telecommunications and computer networks due to cyber-terrorism
- disruption of telecommunications and computer networks by insiders or disgruntled employees

### ***Technical failures and human errors***

Infrastructure owners concentrate on four approaches to minimize threats due to technical failure and human error:

- Training
- Security systems and limited access to vulnerable and critical systems
- External and internal audits
- Systems designed for early detection of errors and rapid recovery

Training programs can reduce human error and facilitate rapid recovery from technical failures and human errors.

*“Training, awareness, and familiarity. Crisis management training. Emergency training.” (Natural gas utility)*

*“Ongoing training and development. Research and analysis on areas that we feel are vulnerable. Hire contractors and consultants and analysts.” (Airport)*

*“Creating an emergency response. Training to prevent or mitigate the incidence. Reviewing company policy and operations to determine if it could be done better or safer.” (Public transportation)*

Security systems and limited access to vulnerable areas and critical systems can reduce the chances for errors.

*“Increase training and passwords. Limited access to terminals.” (Airport)*

*“A lot – training, firewalls, designing systems. Badges and access cards. Structural reinforcements of computer area. Cameras to monitor.” (Long distance telephone)*

*“We have very intensive awareness programs to educate our employees how to secure their workplace. Covers password protection to virus management for our documents. Different rules that go around proper documents. Eliminate access to network. Wearing badges in the building. Different colors for visitors than consultants.” (Cellular telephone)*

*“I know we are very big in information security. We firewall – a system that uses a series of passwords and codes. A person would have to know all the passwords to have complete access. The passwords and codes are changed regularly.” (National commercial bank)*

*“We have password protection. We use the Defender Protector. We have a key in access system.” (Financial market)*

External and internal audits, regulations and standards guarantee adherence to standards and established operating procedures.

*“DOT, OSHA and the EPA do regulatory audits. For an internal audit, we have stations along the pipeline always checking for anything that would stop the flow of gas.” (Natural gas utility)*

Systems that allow for a quick recovery are essential.

*“Insure we have replacement equipment and parts. If computers go down, bring them up as quickly as possible. Try to insure procedures are correct. Know about what can be done so no one can go get into the computer system. Our programming people are a select group. We don’t hire contractors.” (Electric utility)*

*“Everything is duplicated at another site in another state without loss of power grid.” (Bank)*

*“We have a detailed data security program. Very active crisis management program for any kind of loss. How fast you can recover from any loss. Physical security. Access control locking down on desk physically.” (Regional bank)*

*“Automation where possible. Documented procedures which we review annually. Operations integrity management systems. Continuous improvement.” (Oil company)*

*“Network is encrypted all the way from the customer all the way back to his bank. In addition, we have alternative routes or critical telecommunication circuits. Third thing, we have a disaster system that’s running all the time.” (ATM network)*

### ***Physical damage due to terrorists***

Infrastructure owners take several steps to minimize the exposure of their organization to physical damage due to terrorists in the first instance, and to limit the extent of damage should a terrorist strike their infrastructure.

- Minimizing exposure to terrorists
  - Hardening buildings and other facilities
  - Limiting physical access to buildings and facilities
  - Limiting access to computer systems, computer network, and telecommunications systems and networks.
- Controlling the extent of damage should a terrorist strike
  - Hardened facilities to isolate specific functional areas
  - Design systems to be robust and able to rapidly recover from disruptions
  - Redundant systems, including parallel processing or system duplication

However, several executives feel that they face real limits in their ability to protect facilities from terrorism:

*“[We are] not [doing] much. **We are still vulnerable, like all utilities, to the openness of our equipment.** Substations and transmission are not as vulnerable. Internally all our buildings are protected by card access.”*  
(Electric utility)

*“As far as physical damage like to our buildings, with the World Trade Center in mind, our security has taken measures to continually check out buildings, **but there is only so much you can do.**”* (National commercial bank)

*“Extensive security in buildings and card passes. Buildings are protected by security systems. **But a lot of plants are out in the open. There’s not a lot you can do about them but have alternate routes for outside plant [and equipment].**”* (Local telephone)

The following comments, grouped by topic, provide additional details on how infrastructure owners handle vulnerabilities to terrorism.

- Hardened physical facilities

*“Four layers of security: Badges. Computer room. Bullet proof glass. Security guards into complex and then into the building. Structural enhancements. Quake proof. No radio waves in or out. Also sort facilities have videotaped monitoring. Aircraft access is greatly restricted. Badges with hologram sticker, otherwise locks and keys.”* (Overnight delivery)

*“We have a secure building. Guards. Card keys. Locks. Fire protection/water protection. Computer room. Double door system. Blast wall. TV monitor. Six electric feeds. Battery system while switching feeds.” (Financial market)*

*“We have our computers in an undisclosed location (not visible). Double sets of locked doors with no unauthorized access.” (Financial market)*

*“We use security procedures around secure facilities. Card key. Photo badge. Questioning unrecognized persons. Video surveillance. Security personnel. Computer room door lock. Access is by personal code for each employee. Commercial standard for structural things.” (Cellular telephone)*

*“We have security access cards with pictures and no company identification—it would be hard to find. Cameras, guards, badges, three water wells, computer room is isolated, diesel generators with boil systems can go two days on diesel power.” (Internet service provider)*

- Redundant systems and off-site backup

*“Our alternate computer site is miles from the primary site, and we can run our whole network from our alternate site.” (ATM network)*

*“Structured network. Back-up network kicks in too. Mitigates the damage.” (Local telephone)*

*“We have our computers in an undisclosed location (not visible). Double sets of locked doors with no unauthorized access.” (Financial market)*

*“We have Patrol Planes (one engine) that fly just above the pipeline on a regular basis checking for damage - large plant growth, downed trees, anything that might damage the pipe. We have three pipelines that run parallel. They would have to wipe out the whole system to keep the gas from flowing.” (Natural gas utility)*

- Computer security systems to limit access

*“Put in fire walls to protect access to local and wide area networks. Software product to inhibit people from coming through the net. No access through outside links.” (Electric utility)*

*“Limited access. Firewalls. ‘Secure card’ password cycling. All PCs have virus scanners.” (Cellular telephone)*

### ***Disruption of computer and telecommunications systems due to cyber-terrorism***

Infrastructure owners take four types of actions to protect their systems from cyber-terrorists:

- Physical security and limited physical access to key computer and telecommunications operations and facilities.
- Limiting electronic access to computer and telecommunications networks and systems through system design, firewalls, and security codes.
- Software monitoring of system operations and integrity.
- Data encryption of information transmitted over public or quasi-public networks.

Some infrastructure owners, perhaps leading edge companies, appear to feel that firewalls and software protection are just not really adequate to fully protect their systems. The software is not keeping up with the complexity of the systems that need to be protected, and with the sophistication of those who would try to enter and cause damage.

*“Embrace whole system of measures to intercept what’s coming into the network. We have firewalls, **but there isn’t enough software available that really protects us completely. Software just isn’t keeping up.**”*  
(Cable television)

*“**I am very concerned [that] companies can be compromised because of the rapid growth of the Internet.** We are hiring leading-edge consultants for advice and are using encryption more (set of codes and passes). **Firewall protection is just not enough.**”* (Internet service provider)

The following comments, grouped by topic, provide additional details on how infrastructure owners handle vulnerabilities to cyber-terrorism.

- **Physical security.** Physical security and limited physical access to key computer and telecommunications operations are starting points for protecting infrastructures from cyber-terrorism.

*“We’re in a hardened building with double security. You have to go through three doors to get in. Most of our critical systems are underground.”*  
(Electric utility)

*“Perimeter security measures.”* (Natural gas utility)

- **Access prevention.** All infrastructure owners limit access to telecommunications systems, computers and computer networks using firewalls and security codes. Some have eliminated any outside, dial-up links to computer systems.

*“Put in fire walls to protect access to local and wide area networks. Software product to inhibit people from coming through the net. No access through outside links.” (Electric utility)*

*“Limited access. Firewalls. ‘Secure card’ password cycling. All PCs have virus scanners.” (Cellular telephone)*

*“We don’t have a big requirement for outside computer access. Standard ID and password. Dial-back modems to eliminate password protection. Biggest threat is Internet – firewalls, null segments. Hire outside consultant for web site.” (Financial market)*

*“Primarily a system with security checks built in. There is limited access off of our property. We use the Defender System that demands responses and coding. For viruses, we have system detection.” (Public transportation)*

*“Fire walls on some critical systems. We are not as sophisticated as banks and financial institutions. Passwords and firewalls are about it.” (Electric utility)*

*“I know we are very big in information security. We have a firewall – a system that uses a series of passwords and codes. A person would have to know all the passwords to have complete access. The passwords and codes are changed regularly.” (National commercial bank)*

*“Have very rigid internal security of software programs. Firewalls and such.” (Trucking)*

*“We focus on ‘shutting the doors’ so that hackers can’t break in. Firewalls. Proxy server.” (Cellular telephone)*

*“We have a firewall system that is as good as a firewall can be.” (Public transportation)*

*“We have the usual firewalls and gateways. For most sensitive, we have a private network with no dial-in abilities. Cuts down on hackers coming in the way they usually do.” (Local telephone)*

*“Deployed firewalls. Security assessment now [under way]. Filtering in renters. Digital authentication cards. Two-level check. Viruses. Quarterly newsletter points out security.” (Overnight delivery)*

*“We have hired data security experts to find and close any weak links in the system. We also have a lot of firewall protection.” (Airline)*

- **System redundancy.** Redundant networks and systems facilitate recovery from any attempted disruption.

*“Could get in here, but another site would take over without loss of data.” (Bank)*

*“We use redundant networks – Sonet system – which has a looped ring design which reverses information if disruption occurs.” (Cable television)*

*“Redundant systems. Firewalls. Structural enhancements.” (Oil company)*

- **Software controls.** Infrastructure owners also use software controls to monitor the integrity of computer and telecommunications systems.

*“Have an entire logical security department. Refers to network and systems.” (Cellular telephone)*

*“Strong electronic security. All of our systems require an emergency password to get in. Strong internal security measures which we keep improving.” (Internet service provider)*

*“Internal audits and measuring devices to detect line usage and any unauthorized usage.” (Railroad)*

*“The data security program.” (Regional bank)*

*“Security team that monitors systems with the most state-of-the-art equipment.” (Internet service provider)*

*“All the software, hardware, and consultants to test our systems.” (Oil company)*

*“Internal security policy. People inside company constantly monitored. We have access codes to reduce and minimize risk. Can’t say it totally protects, but we use extensive measures to mitigate the possibility.” (Local telephone)*

- **Robust system design.** Design of computer systems and networks to isolate company databases and areas where external customers may have access.

*“All firewall types of protections. Isolate our customer information profiles from content databases (the actual services, e.g. chat rooms). Different processors for different functions.” (Internet service provider)*

- **Data encryption.** Two infrastructure owners—an ATM network and an Internet services provider—mention that they use data encryption to protect the information content of their networks.

*“Data is all encrypted and the encryption key changes every two hours. We also use direct telecommunication private lines.” (ATM network)*

*“[We] are using encryption more (set of codes and passes). Firewall protection is just not enough.” (Internet service provider)*

- **Contingency and recovery planning.** Use of outside consultants and experts to conduct risk assessments, develop prevention plans, and create recovery plans.

*“Task force for latest technology. State-of-the-art security through analysis and consulting. Latest software.” (Airport)*

*Outside firms do risk assessment to make sure we have proper safeguards.” (Railroad)*

*“We have a doomsday ‘worst possible’ scenario with an outside company that backs us up.” (ATM networks)*

### ***Vulnerabilities to physical or cyber-terrorism by insiders and disgruntled employees***

Some infrastructure owners recognize that an insider or disgruntled employee may be the biggest threat to their ability to provide continuous, reliable service despite screening at hiring, technological controls, and good managerial control. These employees have knowledge of and access to systems.

*“If one of our key people goes bad, we are in danger. Control is built in, but we could be hurt from the inside.” (Bank)*

*“We’re vulnerable. Nothing specifically for that.” (Emergency services)*

*“We wouldn’t allow a disgruntled employee to work on our computers. However, disgruntled employees don’t make themselves known.” (Electric utility)*

*“Typical employee won’t hurt much. Any damage would be insignificant, and all data [are] recoverable. Programmers might hurt more. ‘Super-techies’ would do damage, but we change all passwords and key cards and ID. The real risk is the unsuspected disgruntled employee.” (Financial market)*

*“Almost nothing – I don’t know of any business that can guard against that. You might not know they are disgruntled, and you can’t deny your employees access. You didn’t say ex-employees.” (Electric utility)*

*“There is not too much you can do. You can’t change your system completely to be protected. ‘I don’t buy it.’ If a disgruntled employee gains access, he can do serious damage.” (National commercial bank)*

*“Probably the biggest threat ... [We have] limited access to keep systems [secure]. Still, [there is] always someone who has access for some unknown reason.” (Internet service provider)*

*“It’s a matter of damage containment. Gets back to group trust—they have permission to do whatever they want to do and can cause a lot of damage. We have very elaborate real-time surveillance to try and keep damage to a minimum. Within a few seconds, a separate group would know, it provides a check and balance. It’s about all you can do.” (Local telephone)*

Infrastructure owners use a variety of similar methods to reduce if not entirely eliminate the potential for cyber-terrorism by employees.

- Limiting access to critical employees based on job responsibilities
- Human resources and supervisory attention to employee well-being and employee attitudes
- Robust design of computer, telecommunications and operating systems to limit the extent of damage that could occur before detection
- Deny access to former employees by electronic systems such as removing card access, and changing codes and passwords

The following comments, grouped by topic, provide additional details on how infrastructure owners handle vulnerabilities to cyber-terrorism by disgruntled employees and insiders.

- Limiting access to critical employees based on job responsibilities.

*“Most of our employees do not have access to our systems. When key people leave, we block out access as best we can. There is limited access, and we have a system of passwords, codes and firewalls.” (Natural gas utility)*

*“Changing and disabling; passwords. Removal of card access.” (Cellular telephone)*

*“We do restricted access capability based on need to know and job functions of our employees.” (Internet service providers)*

*“Isolate responsibilities - limit capabilities. Good human relations. Revoke access to building systems upon termination.” (Internet service provider)*

*“Lot of internal security. Average person would be stopped by security. Access and badge revocation upon termination.” (ATM networks)*

*“System under locks and keys. If an employee leaves, he is withdrawn from the system. We have different levels of access and directed access.” (Financial market)*

*“Password protection and timely removal if someone leaves.” (Cellular phones)*

*“Everyone has a password for their computer. Nothing else. But MIS people might know of something else.” (Public transportation)*

*“Screening processes. Access control privileges. Negligible consequences – they just couldn’t do much.” (Airport)*

*“We have limited access – priority or need to know. Limited only read as opposed to read and write system. We have public files and private files. We are a little more vulnerable in this area. If someone really wanted to hurt us, I suppose they could do some damage.” (Public transportation)*

*“Critical resources are access trails so that we can detect employee movement on a day-to-day basis.” (Internet service provider)*

*“Security measures. People have limited access as defined by their departments. Just can see the basics. Don’t know all. Some have more access and information than others. Doing this through security software.” (Cable television)*

*“Limited access (electronic or physical) to key elements of the network. Things like limiting people that have access to the network. Multiple employees measuring the different systems – keep tabs on it.” (Local telephone)*

- Basic human resources practices and procedures are key to preventing problems associated with employees.
  - Screening and selecting employees, especially employees with access to critical systems.

*“Screening procedures. Reactive and proactive.” (Bank)*

*“More careful who we hire. Have supervisors keep an eye on any unusual behavior.” (Airport)*

*“Looking into all internal positions of authority in level of access. Every person is being re-evaluated due to a merger - takeover. Because of the merger, we are stagnant at this time.” (Railroad)*

*“Very limited access to critical areas, we observe and monitor behaviors by supervising our employees.” (Electric utility)*

- Managerial awareness of employee attitudes and feelings.

*“Treat our employees right. Competitive severance packages. Security involved if necessary. Badges/access revocation upon termination. Monitoring activity if necessary.” (Oil company)*

*“This is a more difficult issue. If a disgruntled employee is terminated, accounts are closed and locks and passage codes are changed. This is hoping you can catch a bad seed. Company association with employees, security-wise, is based on trust. We are currently ready to implement a new policy to employees outlining company policy and punishment and penalties for disregard of those policies.” (Internet service provider)*

*“Counsel employees.” (Airport)*

*“That’s a tough one. There is just so much you can do. You try to keep your eyes and ears open to employees’ feelings. If you feel there is a problem, we try to act as soon as possible to short circuit a disgruntled employee.” (Public transportation)*

## What are major issues affecting public confidence in infrastructures?

Respondents were asked to indicate what they feel might be the greatest threats to public confidence in their respective infrastructures today and over the next two years. Overall, they cite a common list of threats to public confidence:

- **Terrorism** is seen as a major threat to public confidence in our nation's infrastructures by executives in a variety of industries including banking and transportation. Neither telecommunications nor Internet executives mentioned the threat of terrorism as reducing public confidence in their infrastructures.

*"Terrorists. The picture of Oklahoma City is on everyone's mind. They can't lose that picture. The unknown about the TWA flight." (Bank)*

*"Major threat is terrorism. It's something we're not capable of dealing with right now." (Emergency services)*

*"Terrorism. Terrorist acts at the airports. Airline safety. Deals with airport only not airlines." (Airport)*

*"Terrorist events." (Airport)*

*"Fear from terrorist attacks, better or worse. Depends on how many acts of terrorism there are." (Railroad)*

*"Terrorism is absolutely it." (Cellular telephone)*

*"Terrorism and the ability of the agency to deal with it." (Emergency services)*

*"General terrorism. Fortunately, those kinds of people aren't too smart." (Trucking)*

*"The continued threat of terrorist activity to aircraft." (Airport)*

*"Terrorism and mechanical failure. Better add human error ... unfortunately, I'm afraid the same threats will still be with us in two years." (Airline)*

- Across a variety of infrastructures, executives feel that their ability to provide continuous, quality service increases public confidence, and that, correspondingly, that service outages and interruptions decrease public confidence in their respective infrastructures.

*“Generally confidence in the public politicians is down. I think people aren’t concerned about terrorism. I do remember the radar system going down at the airport; that would shake public confidence. Availability of energy. A disruption of electric service that runs the computer.” (Public transportation)*

*“I don’t see it getting worse. The worst thing that could happen would be an explosion. You remember the apartment explosion in New Jersey? Everybody remembers that, but it happened five years ago.” (Natural gas utility)*

*“Quality of service. Inconsistently perceived in marketplace.” (Cellular telephone)*

*“The biggest threat is not being on time, performance, stuck in traffic jams. We can’t go any faster than the other people. Sometimes the perception is it takes longer and is confusing.” (Public transportation)*

*“Call quality.” (Cellular phones)*

*“Call quality and capacity.” (Cellular phones)*

*“The failure of the agency to perform to its standards. We have very high customer service standards. In our ability to do our job.” (Public transportation)*

*“Interruption of power or energy or inability to restore power would be disastrous to business, or if unable to restore power after a natural disaster.” (Electric utility)*

*“Sudden failures of our operations.” (Long distance telephone)*

*“Service disruption.” (Railroad)*

*“Service disruption. We bring products to consumers. It could hurt economy if there were no deliveries. Ford - Chrysler, U.S. Mail, U.P.S., Ford industry, coal producers, list goes on and on.” (Railroad)*

*“If we started having a lot of difficulties. Right now we don’t have many, and they are fixed quickly.” (Local telephone)*

*“Fear that people can electronically monitor the cellular network. People could have perception that because AT&T broke up into so many companies [that now] there are so many players that there might be some catastrophic event we couldn’t control.” (Local telephone)*

*“Loss of telecommunication. If phone lines go down, we are out of business. Even though we use two different [telephone] companies, there is a lot of sharing of the lines. If they go away, our business will suffer. We all are really dependent on them, dependent on them, even with two companies and dual control.” (ATM network)*

*“The two-week strike – vulnerability in five years for it to reoccur.”  
(Overnight delivery)*

*“Tough question. Can’t begin to answer that. Have to think about that. Major continuous outages would be the single most damaging factor.” (Cable television)*

- **Data security and privacy** emerge as a concern not only for companies dependent on computer networks such as Internet service providers, but also for other infrastructures that use computer networks and the Internet. Implicitly, they appear to feel that a breach of security and trust in any infrastructure that uses computer networks or the Internet will have a broader negative impact on public confidence in many infrastructures.

*“Evolving techno-bandits. They will become a tool for the terrorists.”  
(Cellular telephone)*

*“[We are moving] more into the concept of transaction security. Operate our own shopping isolated from web. Keep Internet separate. Encryption. Pass keys.” (Internet service provider)*

*“Biggest misperception is that we aren’t secure. Biggest problem is the ability for the commercial companies to implement their own security mechanism. It’s technically available but has not been productized. Companies need to buy security solutions—software and hardware. Not enough of them and not complete solutions. There is no reason for this except that government has discouraged solutions requiring encryption.” (Internet service provider)*

*“Unsolicited commercial e-mail or ‘spam’ mail. Customers tell us that they find junk mail in electronic mail boxes – unsolicited mail. Security of cyberspace, electric commerce, will my credit card number be safe?” (Internet service provider)*

*“Complacency and lack of knowledge. Real threats and pressures of the business cause users and management to take risks they don’t understand [for example] putting more information on Internet than they need to. The Internet is growing too fast to provide proper security. I am also surprised by the lack of knowledge by upper management (CEO-CIO). They know they have firewall protection in place but don’t know the risk value of what they need to protect. These same problems could still be around in two years or even four years. The technology is changing so fast, there is no way to keep up with tech issues. A lot of issues are covered and do a disservice to corporate America in the marketplace.” (Internet service provider)*

*“The major threat is transactions over the Internet [and] the accumulation of confidential information – personal and commercial.” (Overnight delivery)*

*“The Internet. Security and authentication will revolve around general confidence of people involved in network security. Part will be about credit card [security], wire transfers, and money floating across networks. We’re seeing a shift, but it will still be a major issue in two years.” (Cable television)*

*“Perceived vulnerabilities in the integrity of the data.” (Bank)*

*“Negative press about the Internet as far as safety and security as a communication medium – erodes public confidence. There are concerns about privacy such as personal information.” (Example: credit card and an e-mail – keeping those personal private memos and financial information secure.” (Internet service provider)*

*“[Wireless communications] will [soon] be digital so confidence should grow.” (Cellular telephone)*

*“I would say privacy issues. Ability to connect. Separation of Internet and Prodigy services. Internet connection mainly. Proxy servers. Different servers that Prodigy uses for connection and caching.” (Internet service provider)*

*“National Security Agency is a huge threat to whole business [for] two reasons. [First, they are] a government agency who thinks they’re chartered with responsibility of information security in U.S. and they’re not. [Second] the NSA more than any other group has kept security solutions out of the commercial sector.” (Internet service provider)*

- The utility industries, particularly the electric and natural gas companies but also the telephone companies, feel that the impact of **deregulation** and opening power generation, transmission and distribution to competition will undermine the primary commitment to customer service that has guided decision-making up to the present.

*Decisions of a business nature as opposed to cyber threats. The [business] market [and especially] deregulation, [but] not cyber terrorism [in our industry]. We're in the middle of deregulation and mass purchasing sales of electricity and gas. (Natural gas utility)*

*[We are] opening up transmission to more economic transfer of energy [however] not enough of the reliability issues are being considered. You could lose your supply of energy. (Electric utility)*

*Concern for deregulation of the electric industry and what that does to public service ... that is the public's main concern. It won't be solved in two years [rather public] concern will be heightened. I believe systems will be less reliable then. The whole industry is struggling with accommodation of electricity transaction in competition. The public doesn't know it but there has been a lot of struggling to provide the needed power. (Electric utility)*

*The trend toward competitive environment. As a regulated company we have the reliable, and [we] set industry product and services and prices. However as we move into a more competitive arena I think customers will begin to lose their confidence in us. Prices will differ as well as product and services. (Electric utility)*

*In the industry, the main concern is market open to competition; which brings in new entrants who may not share the same value or business habits. Analogy – new airlines – some do a good job and some don't. (Local telephone)*

*Whole role of Internet, increasing customer value, so many people access it and using it now. As companies become more competitive, the fear is more cooperation is needed because of the importance of networks but that people like Bell Atlantic and AT&T are less than thrilled to share the information on the front line. But in case of an emergency, they would have to cooperate.” (Local telephone)*

- For certain infrastructures, **environmental issues** are seen as having the potential to have a major impact on public confidence in the infrastructure. It is interesting in this light that none of the electric utilities mentioned issues related to nuclear power generation.

*Environmental [problems]. Community relations in areas where we operate. (Oil company)*

*Oil and [the] press plays it like we're ripping everyone off. Environment should be protected. (Oil company)*

*Military regimes. Operating with unpopular governments. Environmental perception that industry is not doing what it should. (Oil company)*

- The wireless communications industry, but interestingly not the Internet service providers, mention the issue of **fraud**.

*“The major threat is wireless. Cellular fraud – customer’s cellular number is stolen and charges racked up. Have PIN numbers and RE fingerprinting.” (Cellular telephone)*

*“Maybe reduce through other measures. Unpredictable to some degree. It’s low priority for law enforcement (cellular fraud).” (Cellular telephone)*

- The executives at the financial markets and banks focus not on issues of technology or terrorism, but on public **confidence in the financial markets** themselves.

*“Trading futures.” (Financial market)*

*“Fluctuation in stock market. Natural disasters.” (Regional bank)*

*“They’re not technology issues [that affect public confidence. Lack of confidence] comes from the media, from the general perception of our marketplace [portrayed by the media].” (Financial market)*

*“The environment of public trust. The quality of the system and getting good prices. If you lose the system, we have no integrity.” (Financial market)*

*“More and more the public wants the best possible prices. They are very cost and price sensitive. I see that continuing.” (Financial market)*

- The public transit systems see the **availability of funding** to maintain and improve their systems as critical to maintaining public confidence.

*“Available dollars to maintain the system ... it really depends on how far the government goes to support funding for the nation’s infrastructure. It’s becoming a national priority. In an older city like ours, everything needs repairs.” (Public transportation)*

*“The ability to meet the growing needs of the region. Lack of financial resources to meet the needs in a couple of years.” (Public transportation)*

*“Funding. We are supported by tax money. Our wonderful state and federal representatives are always changing funding rules. Our new rail system has been received enthusiastically by the public who want more service and fast.” (Public transportation)*

## What kinds of events have damaged public confidence in infrastructures?

The infrastructures were asked to describe any significant kinds of events that might have damaged public confidence in their infrastructures. These can be grouped into the following categories:

- Short-term interruptions of basic service
- Specific accidents and emergencies
- Areas of possible fraud and deception
- Downsizing

The following comments, grouped by topic, provide additional details on what events are seen as having undermined public confidence in the various infrastructures.

- Infrastructure owners most commonly cited short-term interruptions of basic service as events that undermine public confidence, at least temporarily. These range from outages due to natural events (earthquakes and weather) to basic system failures.

*“In the Western states, the inability for utilities to meet customer demand from wholesale markets. Demand increasing more than supplies. May not build fast enough to handle demand and power may have to be rationed in the future in some way.” (Electric utility)*

*“City flood in 1990 – shut down for a day. Local outage in 1990 – shut down for a half-hour due to electrician cutting wire. No back-up coverage.” (Financial market)*

*“A few minor events – short-term outages. Nothing significant. Coverage in media of undue significance.” (Internet service provider)*

*“We had a clearing problem (the board didn’t clear from one day until the next morning). It was a bad mark on our report card. We lost parts of the trading floor – makes the traders mad as hell. A power outage – if the market goes down, traders are upset, and we have loss of business.” (Financial market)*

*“A large amount of media attention (the result of a power outage), reliability issues for approximately 15 hours which made a media frenzy, small amount of customer inconvenience. The second issue was on changing payment plans from \$3 per hour to a \$20 per month flat rate which tripled our customer usage. This created a large amount of media attention and minimal amounts of client disruption.” (Internet service provider)*

*“Various minor short-term outages. Lack of customer service.” (Long distance telephone)*

*“We have had major weather-related problems within the past 18 months. We had a massive flood in '96. The main subway was flooded, but we had the system up and running in four days. We have had several blizzards. The last one was in April. We were the only transit in the Northeast to be able to operate. It was an inconvenience for people.” (Public transportation)*

- Specific accidents and crises adversely affect public confidence in the ability of an infrastructure to provide reliable service, and to avoid negative impacts on the surrounding communities.

*“Bus wreck. Driver killed and some people injured. Sure affected confidence of our ridership.” (Public transportation)*

*“Incidents with hazardous material. Neighborhoods had to be evacuated.” (Railroad)*

*“Earthquake – three-hour shutdown.” (Airport)*

*“Occasional leaks and spills – environmental impacts.” (Oil company)*

*“The accident where we lost a plane in New Jersey. But that was minimal. Investigation is still ongoing.” (Overnight delivery)*

*“A crash – impact – lost customer confidence.” (Airline)*

*“[Major oil tanker crash and oil spill] was very frightening. [Look] how the rest of the world treated us – like we did this on purpose.” (Oil company)*

- Wireless communications and banking have had confidence undermined by concerns about fraud.

*“Fraud – individual confidences. Call processing failure from software or construction.” (Cellular telephone)*

*“Major fraud – cloning of numbers. Only five percent of the population is affected.” (Cellular telephone)*

*“There was an accusation by customers that they were being misled about stocks sold through the bank – customers thought that money invested in stocks was as safe as other bank money. There was a suit and settlement. Impact – we keep our customers better informed on specifics. We probably lost some customers.” (National commercial bank)*

- Downsizing undermines confidence in the ability of the company to meet its service obligations.

*“The public gets concerned when you downsize – will there be enough people to run things? How will it affect our service?” (Natural gas utility)*

## What actions do infrastructure owners take to reinforce public confidence?

Infrastructure owners appear to be undertaking a common set of initiatives to reinforce public confidence in the ability of their infrastructure to deliver quality, reliable services, and to bolster public confidence when faced with service interruptions or emergencies.

- Build up a reserve of confidence and good will by transparency of company operations and communication with customers and with the community
- Design and operate highly reliable systems, and inform customers and the community about the system
- Quickly and honestly inform customers and the community about service interruptions, outages, or accidents when they occur.
- Rapidly restore service after a service interruption

The following comments, grouped by topic, provide additional details on actions infrastructure owners take to reinforce public confidence.

- Transparency and communication with the public about how the infrastructure operates and what steps it has put in place to provide reliable service is seen as an opportunity to build up a reserve of public confidence.

*“Public education – informing the public of our ability to provide service. Selling ourselves. Confidence is high.” (Emergency services)*

*“We communicate with the community. Radio station. Briefing passengers. Public information. Media protocol.” (Airports)*

*“First thing is to investigate. We have all the details. Prevent misinformation by giving facts.” (Public transportation)*

*“We are openly relentless to commitments to the public. Ad campaigns. Have set up sting operations with police. We are very vocal in media as far as prioritizing the security and privacy of our customers.” (Cellular telephone)*

*“Communicate to the community. Close community ties.” (Cellular)*

*“Track record of service. Community relations – editorials in New York Times. Building roads in Nigeria, for example. Open communications with EPA. Training with police and fire department – drills.” (Oil company)*

*“Continually focused effort to build our networks that limit such failure. Better technology and training. Communicate to customers.” (Long distance telephone)*

*“Demonstrate our level of redundancy. Mission is to be very overt with public. What steps you are taking to correct the problem. Example: A vendor brought the network down. We let the public know what was being done. The quality of our system demonstrates to people our network restoration capabilities. Surveillance, monitoring, resource allocation retrieval, what we do to prevent it from happening again.” (Local telephone)*

- Quick restoration of service after a service interruption or outage, whatever the cause, is viewed not only as a fundamental responsibility, but also is seen as one of the best means of reinforcing public confidence in the infrastructure.

*“Fix it as soon as possible. A lot of the pipeline is underground and more susceptible to floods and farmers. A backhoe is a dangerous machine.” (Natural gas utility)*

*“Try and tell them what’s going on. Announcements to let them know. May have small outages, but when they occur, we try to keep public informed. We try to make it a shorter duration instead of a longer period of time. The whole idea is to maintain the integrity of the bulk power system.” (Electric utility)*

*“We try to be up and going as soon as possible. We do have an electric trolley system that can go out at times. We divert other systems to help lessen the impact. Last winter we had to shut down the bus system for a day because of a huge snow and ice storm. We let people know we were shutting down: A. because of the safety of the public. B. Practicality issue. If we had all our buses stranded, the system would take longer to get running and cost more money to restore. It is like shooting the bullets before the target is available.” (Public transportation)*

- Design and operate highly reliable systems, and inform customers and the community about the system.

*“We have a plan that is followed, and we can sustain under most events.” (ATM network)*

*“We have a reliable system. People always on hand to fix things. Acts of God only. Goodwill with the community.” (Airport)*

*“We have a mirrored site. We had two outages this year, and we were back in operation in five minutes without loss of data. We depend on phone networks. We could lose the New York office and recover through our New Jersey office.” (Banking)*

*“Our network has not gone down. If it did, we would take steps to minimize. We take steps to be proactive instead of reactive. This is a business where prevention goes a long way.” (Internet service provider)*

*“By showing plans to improve our system. We do have a diesel generator with batter backup. If we lose power, the battery backup kicks in until the diesel generator supplies alternate power. Things in the discussion stage – shared backup sites and an industry-wide system.” (Financial market)*

*“We have experienced outages. We had taken steps to protect ourselves with a back-up system, but that failed also. We did a review and implemented more testing of our systems, making sure new locations were protected in a dual way and implementing fault tolerance (no single point of failure).” (Internet service provider)*

*“Gone to having a disaster service so that disruption is minimized. We figure we are available 99.7 percent of the time. We are a form of payment – ATM machines. There’s always an alternative if the machine doesn’t work. You can go to a bank or supermarket and cash a check.” (ATM network)*

*“We have a very positive plan – goal oriented – that we have in place. Host of initiatives that are customer driven. Keeps us on track, no pun intended.” (Railroad)*

- Quickly and honestly inform customers, the community and the press about service interruptions, outages, or accidents when they occur, and about what the infrastructure owner is doing to restore service.

*“If we have, we would have some PR program to tell them what they’re doing about it.” (Natural gas utility)*

*“Notify customer service. Inform customers.” (Cellular)*

*“[In storms and such events it’s real important to let the public know when the power will be restored. We have lots of phone lines. Helps to have a person to talk to and crews that are visible. They need to see that something is being done. If it’s a major disaster, we let them know through the media that we are bringing in crews from as far as a thousand miles away.” (Electric utility)*

*We assess situations and react accordingly. For example, we have hurricanes every year that can affect our main bank and branches. We put ads in the paper and in the media informing people about the situation and what procedures to follow. We take it case by case. Banking sells trust, so we need to be up-front with the public.” (National commercial bank)*

*“We do have service reliability – 99 percent train reliability. We do keep the public informed about any problems and how we are addressing these problems via local papers and television.” (Public transportation)*

*“Try to tell them why and what you’re doing. Communication internally and externally. Open with communications.” (Internet service provider)*

*“Because of the rapid growth we have extended our planning windows. Problem has slowed down a bit giving us more time to catch up and has helped us with this problem. [First] we notify all of our customers if there is a problem. Second we go to the press to help inform them.” (Internet service provider)*

*“When we do have something, we are very forthright to the media. Honesty is always best policy.” (Airport)*

*“Trained all our managers how to improve communication with communities; we present and put forth all information with the highest degree of integrity—good or bad. Establish rapport with all local community government agencies: police, fire, civic. Re-establish disaster training to local communities. (Railroad)*

*“Very important to be able to tell them how long until service is restored. The visibility of where outages are and getting that information correctly out to the media. We are also working on a system where if customers call in on the IVR line we can tell them immediately when their power will be back on. This is still in the development stages. We don’t expect it to be up and running for about two years.” (Electric utility)*

*“That’s part of our extensive crisis management program. Includes media communication. We test that all the time.” (Regional bank)*

*“After an event of any kind, press release, letters to customers of the steps being taken to solve problems, and what is being done.” (Internet service provider)*

*“It’s based on continued communication with the public before, during, and after outages occur. If you tell people what is happening, and what you are planning to do, and what progress you have made, people will understand. As long as they know you are working at it, they are pretty tolerant.” (Public transportation)*

*“If it’s really big, like a hurricane, send out letters, newspapers, television. Let people know what’s being done to fix the problem.” (Local telephone)*

*“We have gone ahead and sent out letters explaining the outage and our plans to correct. Participated in quality programs (Malcolm Baldrige), and ISO 9000 certified.” (Overnight delivery)*

*“Contact each and every customer.” (Overnight delivery)*

*“We would notify customers as quickly as possible about what happened and what we did to restore service.” (Cable television)*

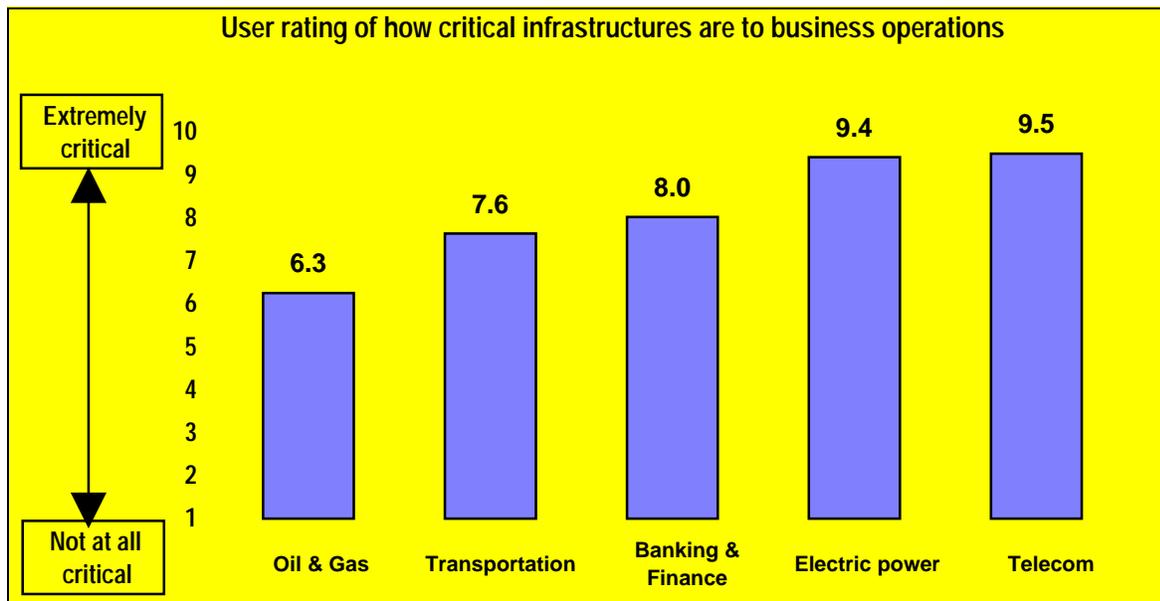
## Discussion: Infrastructure Users

### User perceptions the most critical infrastructure to company operations

#### *Quantitative results*

Business executives resoundingly feel that telecommunications and electric power are the most critical infrastructures to their company operations, followed by banking & finance and transportation. Oil and natural gas are a relatively distant fifth (Figure 18, Figure 19 & Figure 20).

**Figure 18: Perceptions of critical infrastructures (Q7)**  
(Excludes "Don't know" responses; base = 46 respondents)



**Figure 19: Perceptions of critical infrastructures (Q7)**  
 (Excludes “Don’t know” responses)  
 (10 point rating scale where 1 = “not at all critical” and 10 = “extremely critical”)

	Mean	Standard Error of Mean	Standard Deviation	Valid N
Critical system: electric power system	9.41	.15	1.00	N=46
Critical system: gas/oil production, storage and transportation	6.25	.34	2.13	N=40
Critical system: telecommunications	9.49	.12	.82	N=45
Critical system: banking and finance	8.02	.30	1.96	N=42
Critical system: transportation, including airlines, railroads, trucking	7.63	.33	2.20	N=46

**Figure 20: Perceptions of critical infrastructures (Q7)**  
 (Excludes “Don’t know” responses; base = 46 respondents)  
 (10 point rating scale where 1 = “not at all critical” and 10 = “extremely critical”)

	Electric power		Oil & natural gas		Telecom		Banking & finance		Transportation	
	Count	%	Count	%	Count	%	Count	%	Count	%
Not at all critical	0	0%	1	2%	0	0%	0	0%	0	0%
2	0	0%	1	2%	0	0%	0	0%	1	2%
3	0	0%	2	4%	0	0%	2	4%	2	4%
4	0	0%	3	7%	0	0%	0	0%	2	4%
5	1	2%	7	15%	0	0%	5	11%	5	11%
6	0	0%	8	17%	0	0%	1	2%	1	2%
7	0	0%	7	15%	1	2%	4	9%	7	15%
8	7	15%	5	11%	6	13%	9	20%	7	15%
9	8	17%	3	7%	8	17%	10	22%	11	24%
Extremely critical	30	65%	3	7%	30	65%	11	24%	10	22%
Don't know/refused	0	0%	6	13%	1	2%	4	9%	0	0%
Total	46	100%	46	100%	46	100%	46	100%	46	100%

### ***Qualitative comments***

About one third of respondents felt that the electrical power system was the most critical to their company's operation. These organizations tended to be involved with the manufacturing of products or the delivery of services that require materials and supplies (e.g., manufacturing, consumer goods, restaurants/hotels, etc.). To a lesser extent, other industries noted the loss of electricity would be a problem (banking, retail and local telephone).

*"Power. Without that we close down, send people home." (Manufacturing)*

*"If electric power goes down, we are in big trouble." (Banking/Regional)*

The telecommunications infrastructure was the most vital component to about one-third of the respondents. This group consisted primarily of service based companies (e.g., banking and financial services, but also technology companies).

*"Don't know how can choose one. All interconnected. Need all of them. All extremely important. If I had to choose one, I guess it's computers – telecommunications." (Pharmaceuticals)*

*"Telecommunication. The ability for us to use telecommunications to service market sales and manufacture products is essential. If we didn't have phone lines, we would feel pain immediately." (Technology)*

A small percentage, mainly in manufacturing and retail, felt transportation systems were most critical to their operations.

Only two of the survey respondents (both from services-related industries) indicated banking/financial services were the most critical.

### **User confidence in critical infrastructures**

Survey participants were asked to rate their confidence in the ability of five critical infrastructures—electric power, telecommunications, natural gas and oil, banking & finance, and transportation—to provide dependable, reliable service to their company (Figure 21 to Figure 23).

Overall, the business executives surveyed are quite confident in the critical infrastructures that support their business operations.

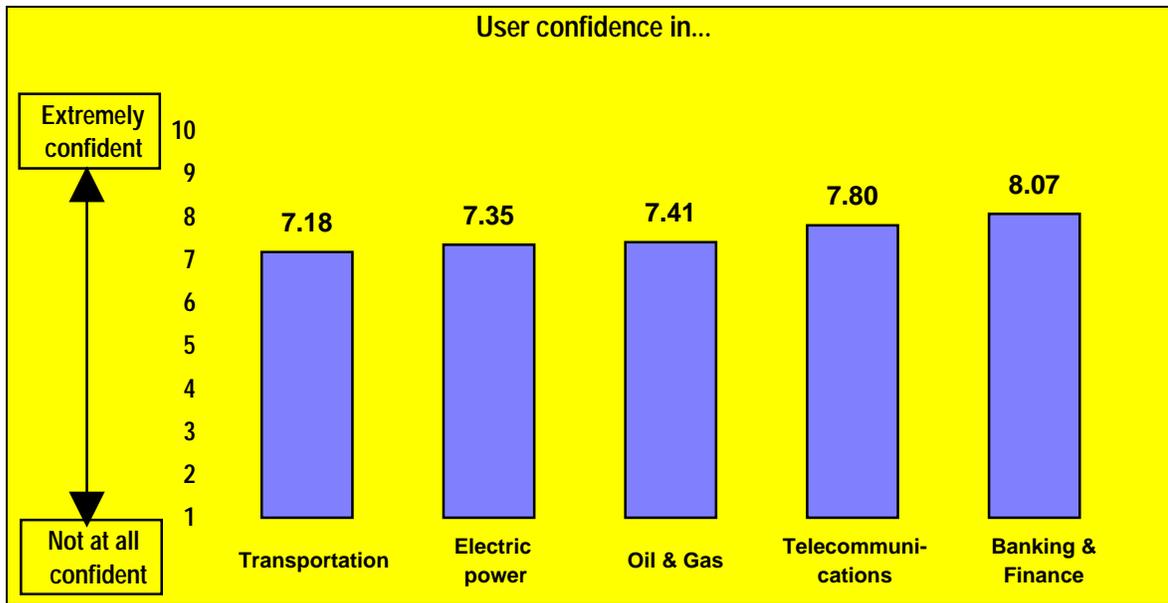
Infrastructure users are most confident in the banking & financial systems (63% rating confidence at 8, 9 or 10 on a 10-point scale where 10 means "extremely confident"; average = 8.07) and in the telecommunications infrastructure (63% rating confidence at 8, 9 or 10"; average = 7.80).

Users are somewhat less confident in the energy production, transportation and distribution systems. Just over half of users (56%) rate their confidence in the electric power systems as 8, 9 or 10 (average = 7.35). A similar percentage (59%,

excluding the “don’t know” responses) rates their confidence in the oil and natural gas systems as 8, 9 or 10 (average = 7.41). Note that, for oil and natural gas, one fifth of respondents answered “don’t know”.

Users are least confident in the transportation systems, including airlines, railroads, trucking, shipping and public transportation. Only 43% of business users rate their confidence as 8, 9 or 10 on a 10 point scale (average rating = 7.18). The lengthy United Parcel Service strike, which covered much of the interviewing period, may have influenced perceptions of vulnerability to disruption of transportation systems.

**Figure 21: Business user confidence in the ability of critical infrastructures to provide dependable, reliable service (Q1)**  
(Excludes “Don’t know” responses; data from Figure 23 )



**Figure 22: Business user confidence in the ability of critical infrastructures to provide dependable, reliable service (Q1)**

(Base = 46 respondents)

(10 point rating scale where 1 = “not at all confident” and 10 = “extremely confident”)

	Electric power		Oil & Gas		Telecom		Banking & finance		Transportation	
	Count	%	Count	%	Count	%	Count	%	Count	%
2	1	2%	0	0%	1	2%	0	0%	0	0%
3	0	0%	1	2%	0	0%	1	2%	0	0%
4	0	0%	2	4%	1	2%	0	0%	2	4%
5	6	13%	3	7%	2	4%	2	4%	2	4%
6	4	9%	3	7%	2	4%	3	7%	11	24%
7	9	20%	7	15%	10	22%	7	15%	10	22%
8	17	37%	11	24%	12	26%	9	20%	13	28%
9	7	15%	7	15%	13	28%	13	28%	5	11%
Extremely confident	2	4%	3	7%	4	9%	7	15%	2	4%
Don't know/refused	0	0%	9	20%	1	2%	4	9%	1	2%
Total	46	100%	46	100%	46	100%	46	100%	46	100%

**Figure 23: Business user confidence in the ability of critical infrastructures to provide dependable, reliable service (Q1)**

(10 point rating scale where 1 = “not at all confident” and 10 = “extremely confident”)

	Mean	Standard Error of Mean	Standard Deviation	Valid N
Electric power	7.35	.23	1.57	N=46
Oil & Gas	7.41	.29	1.74	N=37
Telecommunications	7.80	.24	1.62	N=45
Banking & finance	8.07	.24	1.58	N=42
Transportation	7.18	.21	1.40	N=45

### User perceptions of the vulnerabilities of infrastructures

Business users were asked to rate their feelings, using a 10-point scale (1 = “not at all vulnerable” and 10 = “extremely vulnerable”), about the vulnerabilities of critical infrastructures to four general types of threat:

- Human error or technical failures
- Physical damage due to terrorism

- Disruption of telecommunications and computing networks and systems due to cyber-terrorism
- Disruption of telecommunications and computing networks and systems by disgruntled employees

In aggregate, executives do not feel that critical infrastructures are particularly vulnerable to disruption by technical failures, human error, terrorism, cyber-terrorism or disgruntled employees (Figure 23 & Figure 25).

***Vulnerabilities by type of threat (Figure 25)***

- Telecommunications is seen as most vulnerable to disruption due to technical failures and human errors (average = 5.6).
- Telecommunications, electric power, and natural gas & oil infrastructures are seen as relatively more exposed to threats of physical damage due to terrorism. Banks and transportation systems are seen as relatively invulnerable to the threat of physical terrorism.
- Telecommunications and electric power infrastructures are seen as most vulnerable to disruption due to cyber-terrorism (averages = 5.8 and 5.3, respectively).
- Electric power, telecommunications, and natural gas & oil infrastructures are seen as most vulnerable to disruption due to disgruntled employees (averages = 6.0, 5.9 and 5.5, respectively).

***Vulnerability of telecommunications systems ( Figure 25, Figure 26 & Figure 29)***

- Looking across all four types of threat, the telecommunications infrastructure is seen as the most vulnerable infrastructure. Average ratings of vulnerability to threats exceed 5.2 for all four types of threat. Telecommunications and electric power have the highest vulnerability rating on each threat.
- Telecommunications, as with all infrastructures, is seen to be most vulnerable to disruption by disgruntled employees (average = 5.9), and only slightly less vulnerable to cyber-terrorism (average = 5.8). About one quarter of respondents rated these two vulnerabilities as 8, 9 or 10 on the 10-point scale.
- Telecommunications is seen as least vulnerable to physical damage due to terrorism (average = 5.2).

### ***Vulnerability of electric power infrastructure (, Figure 25, Figure 26 & Figure 27)***

- The electric power infrastructure is perhaps the second most vulnerable infrastructure, following telecommunications. Average ratings of vulnerability to threats exceed 5.3 for three of the four types of threat. Electric power and telecommunications have the highest vulnerability rating on each threat.
- The electric system is felt to be most vulnerable to disruption by disgruntled employees (average = 6.0). Indeed, 33% of respondents rated this vulnerability as an 8 or 9 (but none a 10) on the 10-point scale.

### ***Vulnerability of oil and natural gas production, transportation, storage and distribution (, Figure 25, Figure 26 & Figure 28)***

The oil and natural gas infrastructures are seen as more vulnerable to two types of threat—disgruntled employees (average = 5.5) and terrorism (average = 5.3)—but relatively less vulnerable to cyber-terrorism (average = 4.9) and technical or human failures (average = 4.2).

### ***Vulnerability of banking & finance systems, (Figure 25, Figure 26 & Figure 30)***

The banking & financial system is seen as relatively less vulnerable to failure than other infrastructures.

- Banking & financial systems are most vulnerable to disgruntled employees (average = 5.1), but this is one of the two lowest ratings on this threat.
- Even in the area of cyber-terrorism, banks and financial institutions are not seen as particularly vulnerable (average = 5.0).
- The banking & finance infrastructure is not seen to be vulnerable at all to physical damage due to terrorism (average = 3.7).

### ***Vulnerability of transportation systems (Figure 25, Figure 26 & Figure 31)***

- Transportation systems —airlines, railroads, trucking, shipping and public transportation—are seen as relatively less vulnerable to threats than are most other infrastructures, with average ratings under 5.0 in three of four areas.
- Transportation systems are most vulnerable to disgruntled employees (average = 5.1), but this is one of the two lowest ratings on this threat.

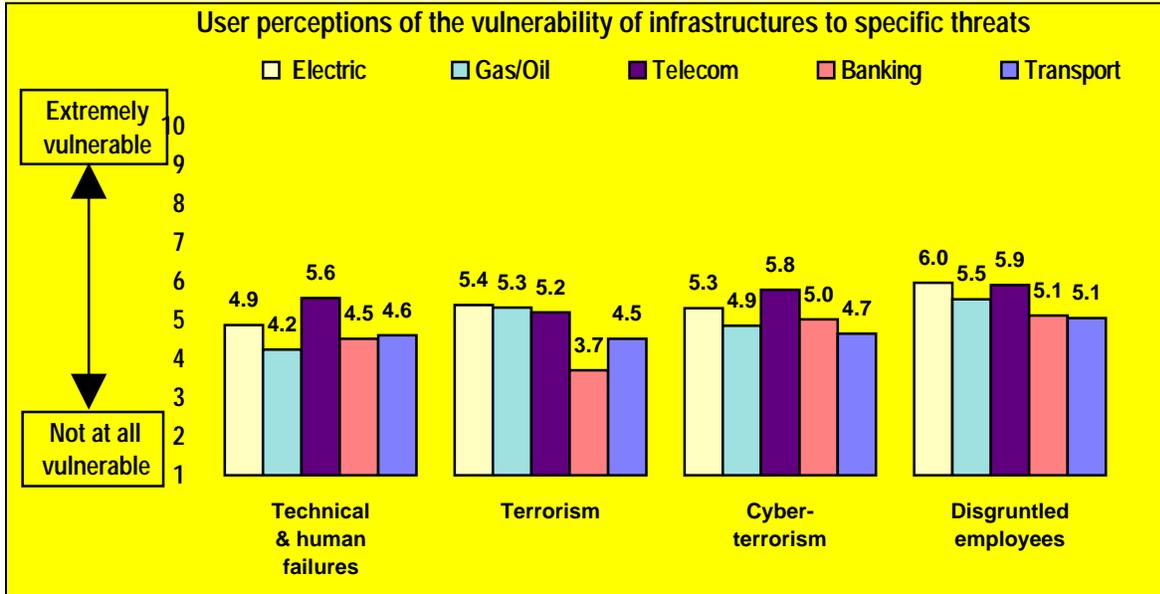
**Figure 24: Business perceptions of the vulnerability of infrastructures (Q2 - Q6)**

*(Excludes "Don't know" responses)*

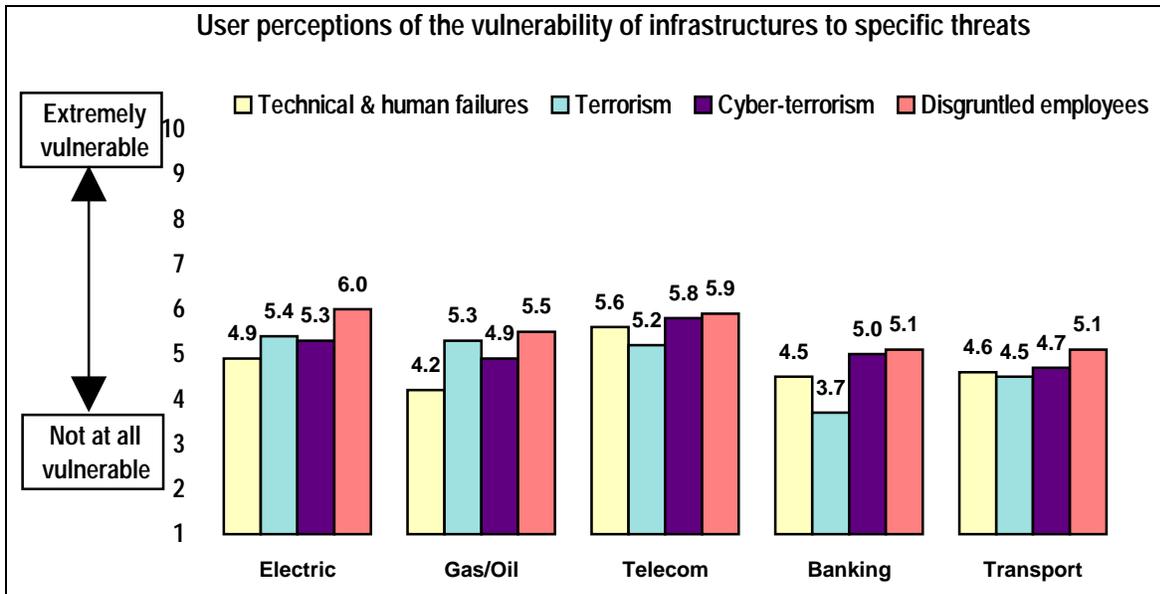
*(10 point rating scale where 1 = "not at all vulnerable" and 10 = "extremely vulnerable")*

	<b>Mean</b>	<b>Standard Error of Mean</b>	<b>Standard Deviation</b>	<b>Valid N</b>
Electric power vulnerable to technical or human error	4.87	.29	1.98	N=46
Electric power vulnerable to physical damage due to terrorist	5.39	.39	2.64	N=46
Electric power vulnerable to disruption of computer/telecomm. due to cyber terrorism	5.31	.35	2.32	N=45
Electric power vulnerable to disruption of computer/telecomm. due to disgruntled employee	5.96	.34	2.29	N=45
Gas/oil vulnerable to technical failures or human error	4.24	.33	2.01	N=37
Gas/oil vulnerable to physical damage due to terrorists	5.32	.42	2.56	N=38
Gas/oil vulnerable to disruption of computer/telecomm. due to cyber terrorism	4.86	.40	2.43	N=37
Gas/oil vulnerable to disruption of computer/telecomm. due to disgruntled employee	5.54	.39	2.39	N=37
Telecommunications vulnerable to technical failures or human error	5.57	.34	2.32	N=46
Telecommunications vulnerable to physical damage due to terrorists	5.20	.37	2.50	N=46
Telecommunications vulnerable to disruption of computer/telecomm. due to cyber terrorism	5.78	.33	2.22	N=45
Telecommunications vulnerable to disruption of computer/telecomm. due to disgruntled employee	5.91	.36	2.38	N=45
Banking vulnerable to technical failures or human error	4.52	.30	1.93	N=42
Banking vulnerable to physical damage due to terrorists	3.71	.33	2.12	N=42
Banking vulnerable to disruption of computer/telecomm. due to cyber terrorism	5.02	.34	2.19	N=41
Banking vulnerable to disruption of computer/telecomm. due to disgruntled employee	5.12	.36	2.32	N=41
Transportation vulnerable to technical failures or human error	4.61	.33	2.18	N=44
Transportation vulnerable to physical damage due to terrorists	4.52	.40	2.68	N=44
Transportation vulnerable to disruption of computer/telecomm. due to cyber terrorism	4.65	.33	2.17	N=43
Transportation vulnerable to disruption of computer/telecomm. due to disgruntled employee	5.05	.35	2.27	N=43

**Figure 25: Business perceptions of the vulnerability of infrastructures (Q2 - Q6)**  
 (Excludes "Don't know" responses; base = 46 respondents)



**Figure 26: Business perceptions of the vulnerability of infrastructures (Q2 - Q6)**  
 (Excludes "Don't know" responses; base = 46 respondents)



**Figure 27: Business perceptions of the vulnerability of electric power (Q2)**

	Electric power vulnerable to technical failures or human error		Electric power vulnerable to physical damage due to terrorists		Electric power vulnerable to disruption of computer/telecomm. due to cyber terrorism		Electric power vulnerable to disruption of computer/telecomm. due to disgruntled employee	
	Count	%	Count	%	Count	%	Count	%
Not at all vulnerable	2	4%	5	11%	1	2%	0	0%
2	6	13%	2	4%	4	9%	5	11%
3	4	9%	6	13%	8	17%	5	11%
4	4	9%	4	9%	7	15%	2	4%
5	13	28%	6	13%	4	9%	5	11%
6	6	13%	5	11%	3	7%	6	13%
7	8	17%	7	15%	7	15%	7	15%
8	2	4%	6	13%	8	17%	10	22%
9	1	2%	2	4%	3	7%	5	11%
Extremely vulnerable	0	0%	3	7%	0	0%	0	0%
Don't know/refused	0	0%	0	0%	1	2%	1	2%
<b>Total</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>

**Figure 28: Business perceptions of the vulnerability of natural gas and oil (Q3)**

	Gas/oil vulnerable to technical failures or human error		Gas/oil vulnerable to physical damage due to terrorists		Gas/oil vulnerable to disruption of computer/telecomm. due to cyber terrorism		Gas/oil vulnerable to disruption of computer/telecomm. due to disgruntled employee	
	Count	%	Count	%	Count	%	Count	%
Not at all vulnerable	2	4%	3	7%	3	7%	1	2%
2	5	11%	5	11%	5	11%	6	13%
3	9	20%	3	7%	5	11%	3	7%
4	7	15%	2	4%	3	7%	2	4%
5	3	7%	4	9%	7	15%	3	7%
6	5	11%	8	17%	1	2%	5	11%
7	4	9%	5	11%	7	15%	8	17%
8	1	2%	5	11%	4	9%	7	15%
9	1	2%	1	2%	2	4%	2	4%
Extremely vulnerable	0	0%	2	4%	0	0%	0	0%
Don't know/refused	9	20%	8	17%	9	20%	9	20%
<b>Total</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>

**Figure 29: Business perceptions of the vulnerability of telecommunications (Q4)**

	Vulnerable to technical failures or human error		Vulnerable to physical damage due to terrorists		Vulnerable to cyber-terrorism		Vulnerable to disgruntled employee	
	Count	%	Count	%	Count	%	Count	%
Not at all vulnerable	1	2%	5	11%	2	4%	2	4%
2	4	9%	4	9%	4	9%	3	7%
3	4	9%	3	7%	1	2%	4	9%
4	9	20%	5	11%	5	11%	5	11%
5	5	11%	6	13%	5	11%	2	4%
6	5	11%	7	15%	9	20%	6	13%
7	6	13%	8	17%	8	17%	10	22%
8	6	13%	5	11%	7	15%	8	17%
9	6	13%	1	2%	4	9%	4	9%
Extremely vulnerable	0	0%	2	4%	0	0%	1	2%
Don't know/refused	0	0%	0	0%	1	2%	1	2%
<b>Total</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>

**Figure 30: Business perceptions of the vulnerability of banking & finance (Q5)**

	Vulnerable to technical failures or human error		Vulnerable to physical damage due to terrorists		Vulnerable to cyber-terrorism		Vulnerable to disgruntled employee	
	Count	%	Count	%	Count	%	Count	%
Not at all vulnerable	0	0%	6	13%	2	4%	2	4%
2	6	13%	8	17%	2	4%	3	7%
3	10	22%	7	15%	9	20%	8	17%
4	7	15%	7	15%	5	11%	6	13%
5	7	15%	9	20%	4	9%	2	4%
6	4	9%	0	0%	9	20%	7	15%
7	3	7%	2	4%	4	9%	4	9%
8	5	11%	2	4%	3	7%	7	15%
9	0	0%	0	0%	3	7%	2	4%
Extremely vulnerable	0	0%	1	2%	0	0%	0	0%
Don't know/refused	4	9%	4	9%	5	11%	5	11%
<b>Total</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>

**Figure 31: Business perceptions of the vulnerability of transportation (Q6)**

	Vulnerable to technical failures or human error		Vulnerable to physical damage due to terrorists		Vulnerable to cyber-terrorism		Vulnerable to disgruntled employee	
	Count	%	Count	%	Count	%	Count	%
Not at all vulnerable	1	2%	4	9%	3	7%	2	4%
2	8	17%	11	24%	4	9%	5	11%
3	7	15%	5	11%	9	20%	6	13%
4	6	13%	3	7%	4	9%	4	9%
5	8	17%	4	9%	9	20%	8	17%
6	6	13%	7	15%	3	7%	5	11%
7	2	4%	2	4%	6	13%	5	11%
8	3	7%	4	9%	4	9%	6	13%
9	3	7%	2	4%	1	2%	2	4%
Extremely vulnerable	0	0%	2	4%	0	0%	0	0%
Don't know/refused	2	4%	2	4%	3	7%	3	7%
<b>Total</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>	<b>46</b>	<b>100%</b>

**What would be the effects of an infrastructure failure?**

Survey respondents were asked to identify how long their company could survive a disruption of services by an infrastructure, and what would be the most significant effects of the failure.

***Electric power system***

***Length of time before substantial impact on operations***

A small number of companies noted that a failure or serious disruption of electric power would not create a crisis situation because of the presence of back-up power systems.

*“Wouldn’t affect [our] operating center; the building [is] designed not to lose power, [it is] a very advanced operation, and can go 60 days [without outside power supply]. Corporate [headquarters would stop] immediately.”  
(Financial services)*

*“Indefinitely because of alternative resources. Our major [facility] has a battery turbine engine back up, and if that fails we have second site 3,000 miles away.” (Banking/National)*

*“A minimal amount of time because we have an UPS [Uninterruptible power supply] provider and back-up systems in place.” (Local telephone)*

Approximately one-half estimated that an electric outage and crisis situation would substantially affect their operations in **less than 24 hours**. Of this group, most were involved in manufacturing. However, banking/financial, technology, retail and restaurant concerns could also be in crisis situations quickly.

*“Can’t function.” (Manufacturing)*

*“Restaurant would shut down.” (Restaurant/hotel)*

*“Twelve hours - computer ordering systems down; freezer and cooler would reach danger point.” (Retail)*

One-third felt their operations could continue in some capacity for **more than one day but no longer than one week** if they were to experience a full electrical outage. Service companies (financial, technology and retail) seemed to have the ability and back-up systems to allow themselves to function for a few days to a week. Different manufacturing operations had shorter time horizons.

*“I guess different divisions of the company would impact differently. We are in the data center. We have back up systems and could operate without electric four or five days. Other departments could not operate as well as we could not sell product, we would have loss of sales and revenue.”  
(Publishing/Broadcasting)*

*“Few days. Time becoming increasingly shorter and shorter. Back-up systems cost money. We have been reducing redundancy and it leaves us more vulnerable. Not stockpiling products. Stockpiles are diminishing.”  
(Pharmaceuticals)*

Many companies, again mainly producers of consumer goods, noted that the effects would be felt nearly immediately and would result in some degree of lost business and/or sending production workers home.

*“Out of business four hours later. Some fallout - less than 10% failure rate.”  
(Manufacturing)*

*“Out of business – can’t receive orders or fill on timely basis. All systems are interconnected. All are done on computers today. If you have no stockpiles – no business.” (Pharmaceuticals)*

*“If it hit our plant, that’s a disaster. If corn flakes were on the line and it stopped, it’s a huge clean-up problem. Computer would be a bigger problem. Couldn’t communicate with our customers.” (Consumer products)*

Less than one in five estimated the effects would be reduced somewhat due to back-up systems. While these companies tended to be manufacturing, they were mainly exceptions to the overall feelings of manufacturers.

*“We have backup power—some capacity but not much.” (Manufacturing)*

*“Would cut production in half (50 percent). Revenue and profitability would be cut by more than 50 percent.” (Consumer products)*

*“Operating center can go for 60 days. Corporate loss of power, no generator, no computer, no business.” (Financial services)*

Due to back-up systems, some financial services and other service-oriented providers (4 respondents) noted the effects would be minimal.

*“Would be minor. Have alternate power source.” (Financial services)*

*“Wouldn’t affect [our] operating center; the building [is] designed not to lose power, [it is] a very advanced operation, and can go 60 days [without outside power supply]. Corporate [headquarters would stop] immediately.” (Financial services)*

*“Indefinitely because of alternative resources. Our major [facility] has a battery turbine engine back up, and if that fails we have second site 3,000 miles away.” (Banking/National)*

### **Gas and oil production, storage and transportation**

*Length of time before substantial impact on operations:*

Direct dependence on natural gas and oil appears to be less critical to most companies. Only two respondents (both manufacturers) believed their operations would shut down in **less than 24 hours** with oil or gas production, storage or delivery.

*“Eight hours.” (Manufacturing)*

Two-thirds of the companies felt their companies could function between **two days to two weeks** without gas or oil production/storage or transportation. Lower thresholds were indicated by manufacturing operations.

*“Two weeks.” (Financial services)*

*“Two days probably.” (Consumer products)*

Nearly one-quarter indicated a gas or oil delivery problem would have ***little to no effect*** on their operations.

### ***Effects of infrastructure outage on business operations***

Over one-half of the companies responding felt problems with gas or oil production, storage or transportation would cause some kind of slow down in the delivery of their goods or services. The effect lies not so much with the production line as with several critical forms of transportation: the delivery of raw materials, the shipping of finished products, the movement of service trucks, and most importantly, the inability of employees to get to work.

*“Wouldn’t be able to acquire materials and eventually stop production.”  
(Manufacturing)*

*“If trucks don’t run, products and parts don’t get delivered. If cars can’t run, people can’t get to work.” (Technology)*

*“Customer dissatisfaction. Can’t open doors without heat.”  
(Banking/National)*

Many respondents did not seem to feel a gas or oil disruption would affect their operations much. Most of this is credited to back-ups or alternative sources of energy.

*“No complete stop. We have back ups. It would be minor and workable, reallocate energy.” (Manufacturing)*

*“Our industry is not reliant on it and we have backup suppliers.”  
(Manufacturing)*

Few (10%) felt this would cause an immediate or short-term halt in operations.

*“This is critical. Delivery would be down 30 percent.” (Consumer products)*

*“People would have to work remotely – at home. A limited number of people could make it to the workplace, but then we could have a hectic problem.”  
(Technology)*

### ***Telecommunications***

*Length of time before substantial impact on operations:*

All respondents felt that a failure or major disruption of telecommunications would have a significant impact on business operations. However, companies were nearly evenly divided on their assessment as to whether a crisis would develop in less than 24 hours or if they could continue for a longer period of time.

- Less than 24 hours:

*“Immediately.” (Financial services)*

*“Enormously severe. We are a wireless industry.” (Manufacturing)*

*“If we lost our telecommunications, it would be devastating.” (Local telephone)*

*“We could recover within eight hours depending where the system broke down. We redirect lines and have back-up systems set up.” (Banking/Regional)*

- Longer than 24 hours:

*“Two days.” (Restaurant/hotel)*

*“After 24 hours, data goes down; after 72 hours, we’re crying.” (Retail)*

### ***Effects of infrastructure outage on business operations***

Less than 20% of the companies participating indicated a telecommunications shutdown would only minimally affect their business. This sentiment was due to the fact they felt back-up plans would cover them.

Eight of 10 companies noted considerable negative effects would occur if their telecommunications system went down. Situations varied, but not necessarily by industry.

- Disruption of sales and customer service:

*“We can’t sell. Sales and delivery.” (Manufacturing)*

*“Service to planners and customers would cease. Completely affect our business.” (Financial services)*

*“No customer orders could be sent.” (Retail)*

- Supplies would be halted:

*“Supplier problems.” (Restaurant/hotel)*

*“No shoes in the stores.” (Retail)*

- Multiple locations and functions are interconnected:

*“Couldn’t place orders. Impact our ability to design our products. Impact our ability to service our product in the field. Large equipment.” (Manufacturing)*

*“Because systems are interconnected, can’t receive or fill orders, can’t pay bills. We are worldwide – normal business would be totally disrupted.” (Pharmaceuticals)*

*“Unable to process credit card transactions and unable to provide our product. Our operations would shut down.” (Financial services)*

- Company's reputation and customer perception would be damaged:

*"Critical thing is not the time as much as it's a privacy issue and integrity of our business. If Pacific Bell goes out for a day we would be all right; beyond [that] it will be an enormous inconvenience as opposed to electric power which would stop us altogether. We do have redundancy systems."*  
(Manufacturing)

*"We link up our computers through their lines. Orders would all be gone. Would have an immediate financial impact. Couldn't service our customers."* (Consumer products)

*"The process would prohibit us from exchanging information and our customers would not have access to our branches and ATM machines."*  
(Banking/Regional)

### **Banking and finance**

*Length of time before substantial impact on operations:*

Very few companies felt that a disruption of banking and financial services would adversely affect operations in the short term.

For about two thirds of companies across several industries, the disruption of banking or financial services would affect operations somewhere between two days and two weeks.

*"Five days." (Restaurant/hotel)*

*"Ten days." (Pharmaceuticals)*

*"Two days." (Manufacturing)*

The remainder indicated they could continue with little or no adverse affects in regard to this type of disruption, without specifying how they could continue.

*Effects of infrastructure outage on business operations:*

The major issues noted across all industries participating in the survey centered around three themes: the inability to access funds or loans, the impossibility of conducting a variety of transactions, and a halt in their ability to **efficiently** conduct transactions.

- No access to funds:

*"Couldn't pay people—they'd leave." (Restaurant/hotel)*

*"Cash flow disrupted. Couldn't secure short term lending instruments to supply warehouses." (Retail)*

*"No payments to vendors." (Consumer products)*

*“Would affect paying bills and could not deposit customer payments.”  
(Direct marketing)*

- Disrupt electronic transactions:

*“We wouldn’t be able to communicate with other banks that we deal with.  
Can’t transmit funds (money) between various financial institutions.”  
(Banking/National)*

*“Inability to exchange information with Federal Reserve Banks and other  
financial institutions.” (Banking/Regional)*

### ***Transportation (airlines, railroads, trucking and overnight delivery)***

*Length of time before substantial impact on operations:*

In this area, responses varied by industry. Companies feeling a disruption in transportation would affect them quickly (two days or less) tended to be manufacturers and consumer products companies (approximately one-third). The majority of respondents felt they could operate on a longer term without various modes of transportation. Several service-oriented companies not involved in the delivery of the product noted that a disruption of transportation infrastructures would not directly affect their operations.

- Immediately (2 days or less):

*“Twenty-four hours on trucking.” (Manufacturing)*

*“One day.” (Retail)*

*“Two days.” (Consumer products)*

- Longer term:

*“Five days.” (Restaurant/hotel)*

*“A week.” (Retail)*

*“One week.” (Technology)*

*Effects of infrastructure outage on business operations:*

While the time interval may vary by industry before the disruption of transportation affects company operations, few industries would not be affected at all by disruption of transportation.

- Manufacturing/Consumer Products:

*“Can’t deliver products.” (Manufacturing)*

*“That’s how we get our parts and deliver our products to our customers.  
Without it we don’t invoice.” (Manufacturing)*

*“Product not able to go out. Shipping occurs daily.” (Consumer products)*

*“We need to move our product and raw materials. We have seven to ten days of inventory but two days would put us in trouble.” (Consumer products)*

- Food

*“No product.” (Restaurant/hotel)*

*“Unable to supply our retail food stores.” (Retail)*

- Financial Services/Banking

*“People in field offices wouldn’t get suppliers or documents.” (Financial services)*

*“Delivery of statements delayed. Delivery of other institutions checks and deposits delayed. Lost dollars due to non-investment.” (Banking/National)*

## **Major concerns about infrastructure failures**

Nearly two thirds of participating executives indicated their greatest concern revolved around the failure of their telecommunications or electronic information networks due to either service outages, security breaches by hackers, planned cyber-terrorism or disgruntled employees. They did not feel that there were any differences between their short-term and longer-term concerns.

*“Telecommunications. The ability of the major companies (AT&T, SWB, Sprint, MCI) to secure their network and plan for failures.” (Banking/National)*

*“In our case, we put a lot of emphasis on disruption by hackers, disgruntled employees or human error. So biggest concern is telecommunication and data processing, our MIS System.” (Manufacturing)*

*“Speaking about my own company, the combination of telecom and power is our life blood. The thing we worry about most is electronic cyber terrorism. These people are very smart. We are spending more and more time with the FBI and Secret Service instructing on computer terms and services.” (Banking/National)*

*“Potential failure of telecommunications; would have long-lasting affect. An attack on the telecommunications system would cause immediate disruption to my company.” (Technology)*

*“Systems integrity issues, on how viable accessing them is. Security and Integrity.” (Financial services)*

*“Telecommunications because of the increasing need to communicate with our many locations and the demands put on the telecommunications and computer infrastructure.” (Retail)*

*“The proliferation of telecommunications providers further degrades our ability as a nation to coordinate all security intrusions be they cyber or electronic, and the need to recognize unauthorized, intrusive cyber attacks.” (Local telephone)*

As would be expected, electrical power outages were also a major concern for about one fifth of the companies.

*“We had two major power lines down. One line only feeding our center.” (Financial services)*

*“A major electrical power failure – we have emergency generators for 72 hours – then we would be useless.” (Restaurants/Hotels)*

Transportation was noted as the greatest concern for a handful of participants.

*“Transportation. ‘UPS thing,’ can’t deliver fresh fish so may have to shut down.” (Restaurant/hotel)*

*“I would say for very short term—trucking (in light of the UPS strike) can be very disruptive.” (Retail)*

A few participants also noted some other potential concerns.

*“Disruption of diesel oil gasoline supplies or hike in price.” (Retail)*

*“Banking and finance.” (Consumer products)*

*“Gas and oil system breakdown.” (Consumer products)*

## **How have infrastructure failures affected companies**

About three quarters of respondents indicated that their companies had experienced an infrastructure failure within the past year.

More than one-half of the disruptions were related to electric outages. As would be expected, the outages covered all industries. The impact of electric power outages varied not only by industry, but within industries as well. Most resulted in temporary work stoppages ranging from several minutes to several hours. Longer delays often entailed sending employees home.

Electrical outages caused minimal interruptions:

*“Transformer went down—were able to remain open.” (Retail)*

*“It was electrical but we were able to recover immediately so we didn’t experience any downtime. Customers probably were not aware there was a problem.” (Banking/Regional)*

*“Electric power – had to shut down operations for brief periods.” (Technology)*

*“The electric system goes down on occasion, but only for very brief periods. It affects our company minimally.” (Banking/Regional)*

Electrical outages involved sending employees home:

*“Power - safety systems back up. Send people home. Four hours of reduced operation.” (Manufacturing)*

*“Had a couple of power outages - lights go out, etc. People go home - we stop manufacturing and engineering. Talcum outages - but only an hour or two - that’s serviceable.” (Manufacturing)*

*“Electric. We had to close shop for the day.” (Retail)*

*“Just last week we had a power failure. People had to go home. We had UPS [uninterruptible power supply] back up for our computer system. We didn’t lose any data, but it stopped operations for the day. The telecommunications provider has had some back-haul problems. Took down a whole area for a day.” (Technology)*

*“Complete stop.” (Manufacturing)*

*“1. Power failure. Had to send people home after a few hours. 2. Telecommunications, didn’t have to send people home, but it stops business. 3. UPS strike was more expensive for us. Had to find new vendors and it costs more.” (Technology)*

Concerns with telecommunications or computer system interruptions seemed to center around the inability to communicate with customers and the resulting loss of confidence, customer satisfaction or ultimately the loss of business.

*“Electrical power outages, storms, late processing take place. Telecommunications - no voice mail for customer support - customer dissatisfaction.” (Banking/National)*

*“We have had telecommunication failures (twenty-four hours) but not across the board (not a complete break down). It disrupted service but not loss of sales and revenue due to a prolonged disruption.” (Publishing/Broadcasting)*

*“Nothing nationally – but we had a computer system down for 48 hours affect our reservations – people coming in – people leaving – they were pretty understanding. I don’t think [it] affected us in a major way.” (Restaurants/Hotels)*

*“We had loss of sales and service and lack of customer commitment due to loss of our product – customers went somewhere else.” (Technology)*

Some companies noted the impact of the UPS strike, and their perceptions of the impact of disruptions of the transportation infrastructure.

*“Electric – cutbacks in business – loss of communication. **UPS strike – loss of revenue and increase in expenses.**” (Consumer products)*

***UPS strike was more expensive for us. Had to find new vendors and it costs more.*** (Technology)

*“We have had some electrical interruptions. In some (not all), if natural gas is shut down, we can switch to oil. **In transportation, we had a strike. We were forced to find an alternate way of getting our product to market.**” (Consumer products)*

## **Elasticity: perceptions of the impact of events and practices on confidence in infrastructures**

In order to estimate the impact that certain types of events would have on the confidence of business customers in an infrastructure, respondents were asked to indicate whether they felt that a certain set of events would strongly increase, slightly increase, neither increase nor decrease, slightly decrease or strongly decrease their confidence in the ability of the infrastructures to provide continuous, reliable, high-quality products and services.

Overall, the ratings by infrastructure users are nearly identical to those provided by infrastructure owners. Infrastructure users are slightly more likely than owners to feel increased confidence if an infrastructure can demonstrate its ability to recover from a failure, or to resist cyber-terrorism.

### ***Events that are perceived as increasing confidence in infrastructures***

Executives feel that company practices, procedures and operational reliability have the strongest positive impact on their confidence in infrastructures (Figure 11 & Figure 12; see also Figure 37 & Figure 38).

- ***Contingency or emergency planning and preparation*** lead all other actions in increasing business confidence in infrastructures including, it is interesting to note, proven reliability. Regular rehearsal of a backup plan (68% “strongly increase”) and presence of backup systems (55% “strongly increase”) are the two leading factors that increase confidence.
- ***Proven reliability*** in providing services also stands out as an extremely strong factor enhancing confidence (53% “strongly increase”). We can speculate that proven reliability is a cost-of-entry for an infrastructure

provider, but that the ability to handle crises and system failures differentiates among infrastructure owners.

For business users, knowledge that an infrastructure computer system can resist a computer hacker also strongly increases confidence. For infrastructure owners, this type of event received more mixed ratings.

- **Transparency** of company operations and planning is viewed as critical. The companies feel that infrastructure owners should inform business customers about their operations.
- **Adherence to an external audit or standard** established by a legitimate authority, such as an industry code, can also be powerful guarantee.

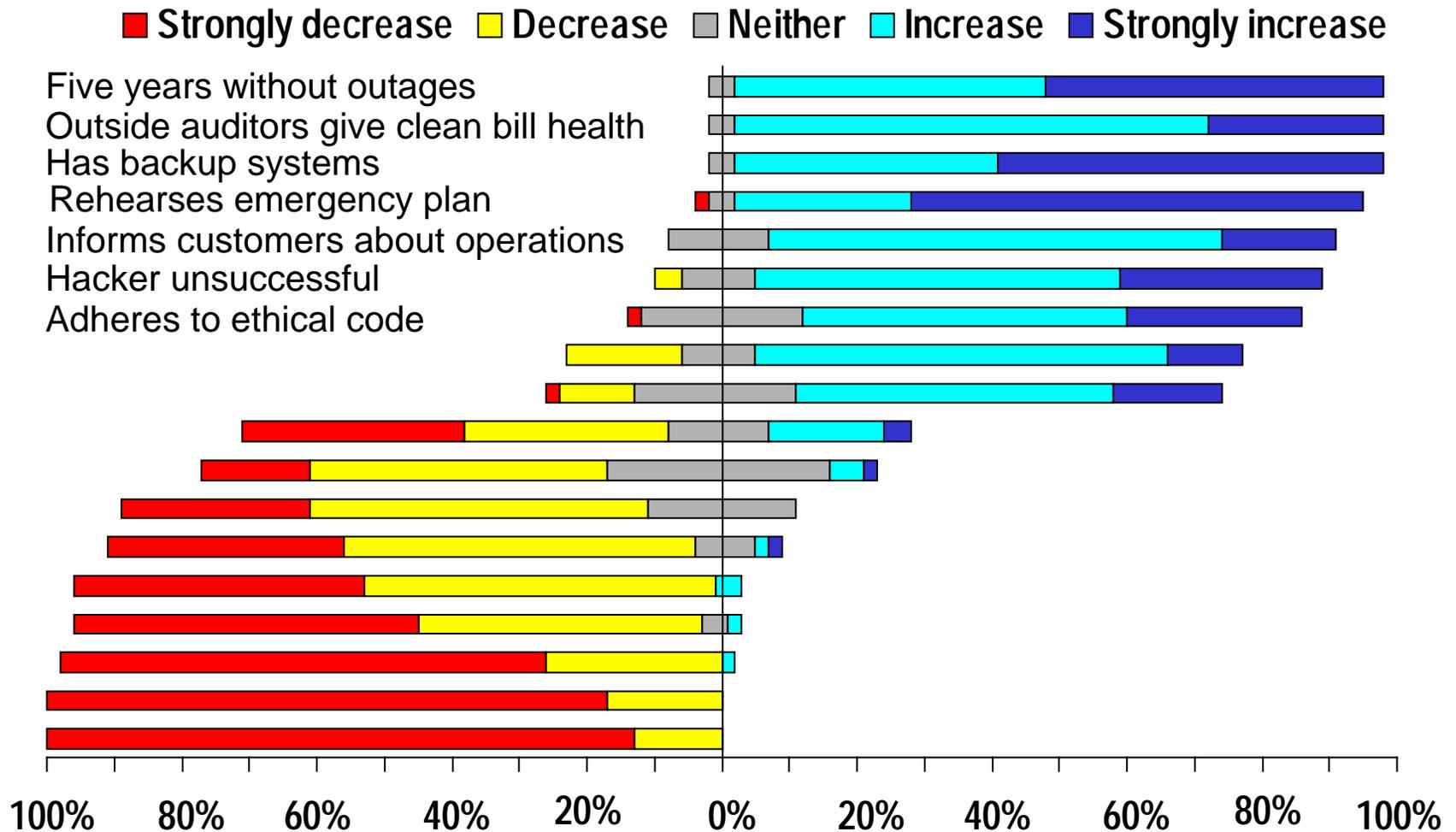
**Figure 32: Events that are felt to increase confidence in infrastructures**

The company...	“Strongly increase” or “slightly increase”	
	Users	Owners
Reports no service outages in five years	96%	97%
Has backup systems in place	96%	98%
Outside auditors give company a clean bill of health	96%	93%
Rehearses emergency response plan	93%	90%
Informs business customers about operations	85%	99%
Hacker unsuccessful at entering computer system	85%	63%
Voluntary adhesion to ethical code	74%	91%

***Figure 33: Events that are felt to increase confidence in infrastructures***

[Insert PowerPoint slide here]

# Figure 33: What factors increase business user confidence in infrastructures (Users)?



### ***Events that are perceived as decreasing confidence***

Corresponding to the results in the previous section, executives feel that a lack of recovery planning, lack of transparency, failure to meet standards and regulations, and operational failures are the most significant factors that would decrease their confidence in infrastructures (Figure 13 & Figure 14; see also Figure 37 & Figure 38).

- ***Lack of recovery planning.*** Users feel that the absence of backup systems and emergency plans to recover from system failures would be among the most important factors reducing their confidence in infrastructures.
- ***Lack of transparency.*** Failure to inform business customers about operations, and, most of all, deception strongly diminish the confidence of business customers.
- ***Failure to meet standards and regulations for operations,*** for example, when outside auditors find security or reliability problems, or the company is fined for violating a regulation, are seen as decreasing customers confidence.
- ***Operational failures,*** such as a successful entry into a computer system by a computer hacker, a major outage caused by a computer system failure, or a record of periodic service outages decrease confidence in the ability of an infrastructure to deliver services reliably and dependably.

The ratings given by infrastructure owners and users are nearly identical. The most significant differences occur in the following areas:

- In the area of failing to inform business customers about operations, infrastructure users are more likely to feel lowered confidence (78%) than owners would expect (69%).
- In the area of periodic service outages with service restored rapidly, users are more likely to feel lowered confidence (63%) than owners (58%).
- Owners are far more sensitive to fines for regulatory violations (89%) than are users (56%)

**Figure 34: Events that are felt to decrease confidence in infrastructures**

---

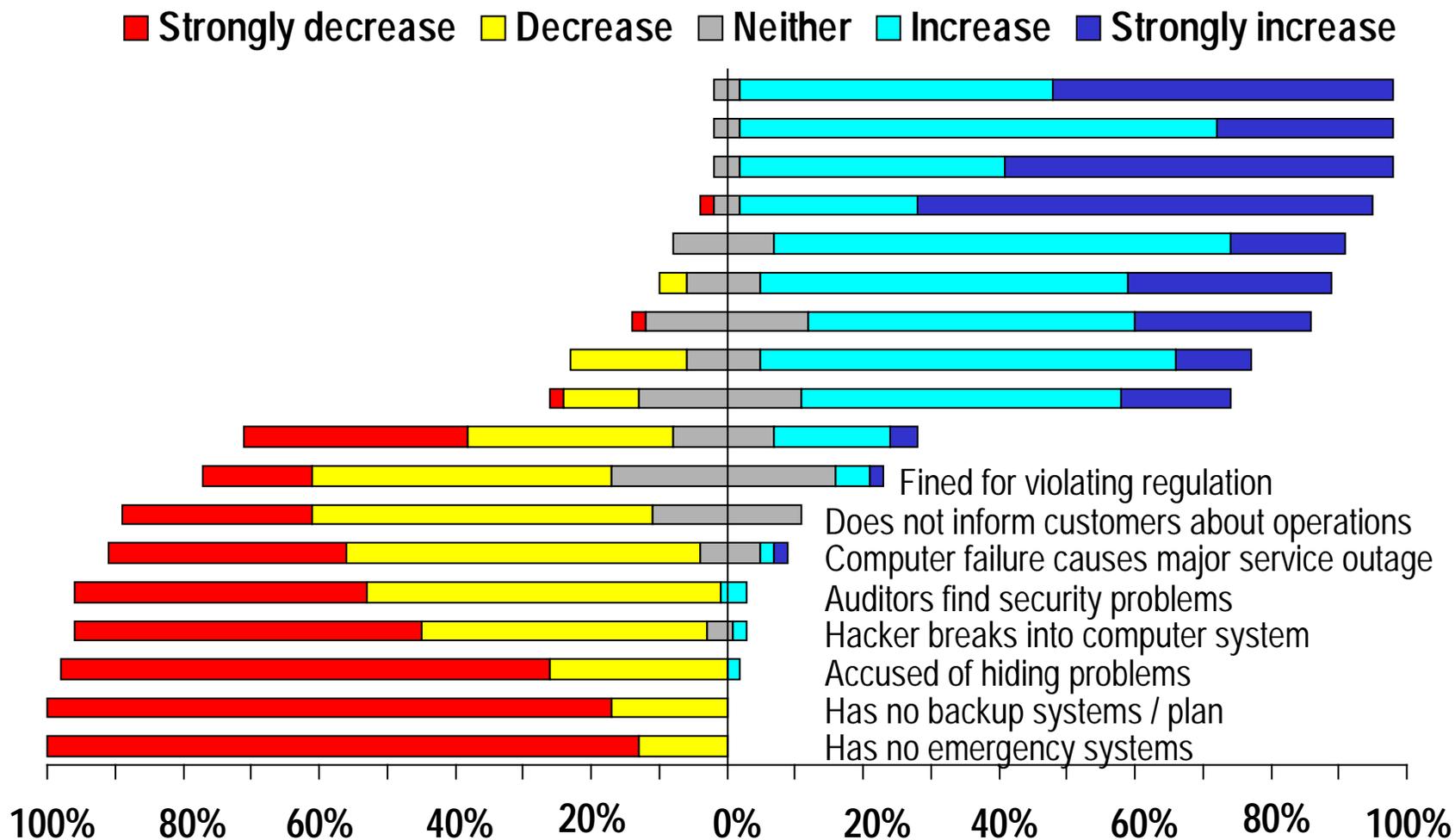
	<b>“Strongly decrease” or “slightly decrease”</b>	
	<b>Users</b>	<b>Owners</b>
Company has no backup systems	100%	96%
Company accused of hiding problems	98%	100%
Company has no emergency systems	98%	96%
Auditors find security/reliability problems	96%	97%
Computer hacker successfully enters system	91%	92%
Computer failure causes major outage	87%	88%
Company does not inform business customers about operations	78%	69%
Record of periodic service outages but service is restored rapidly	63%	58%
Company is fined for violating a regulation	56%	89%

---

***Figure 35: Events that are felt to decrease confidence in infrastructures***

[Insert PowerPoint slide here]

# Figure 35: What factors decrease business user confidence in infrastructures (Users)?



***Events that are perceived as having mixed effects on confidence in infrastructures***

Three events have mixed effects on the confidence of business customers in infrastructures. These events have in common the fact that they involve the identification of infrastructure problems on the one hand, which would tend to decrease confidence, but also involve the elaboration of a plan to rectify those problems, which would have the effect of increasing confidence (Figure 36; see also Figure 37 & Figure 38).

Two events generally increase confidence, but decrease confidence for some:

- Company identifies problems and announces a plan to resolve those problems within one year
- Government enforces minimum standards for reliability

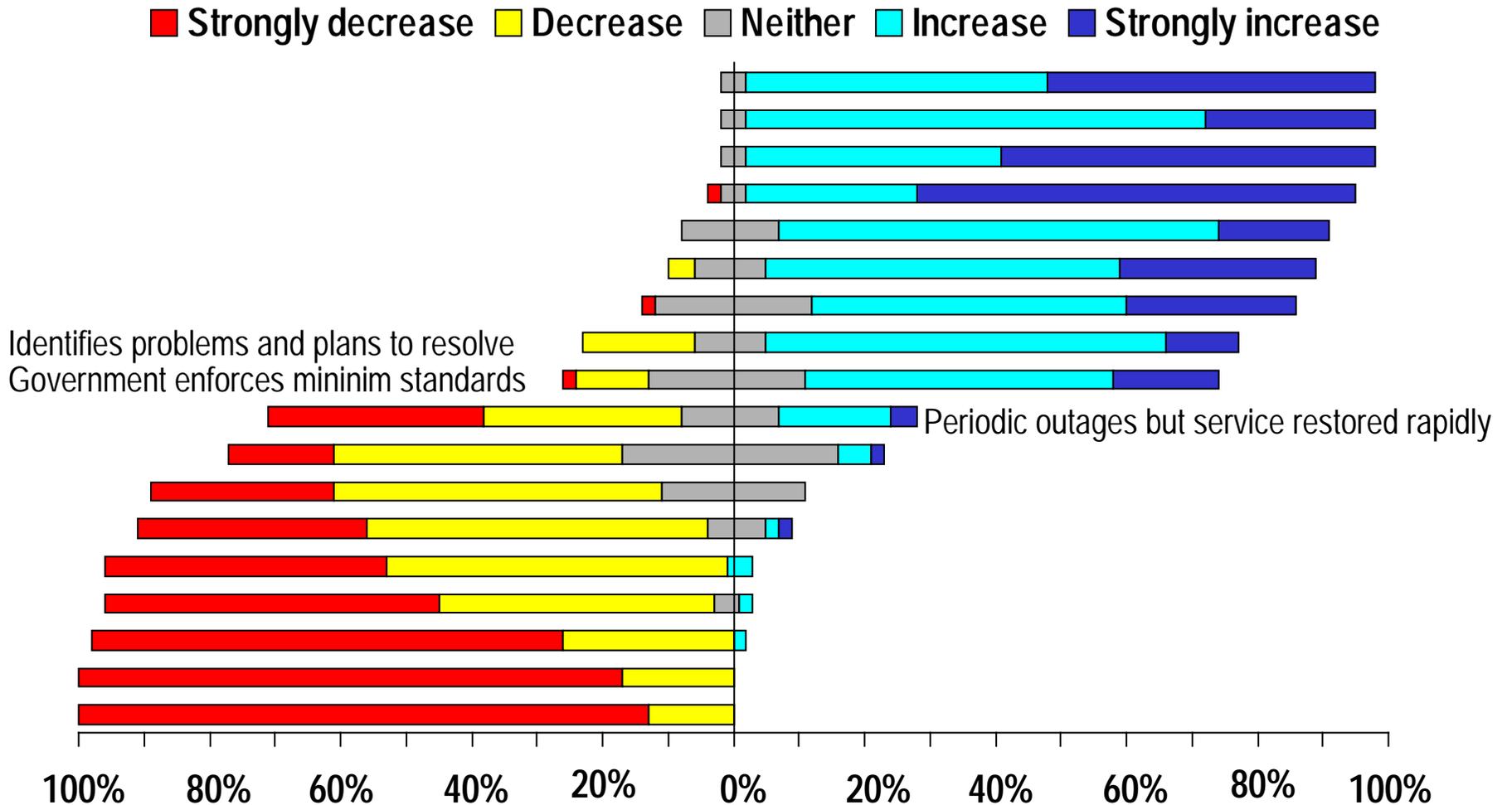
One event generally decreases confidence, but increases confidence for some:

- Company has a record of periodic service outages, but restores service rapidly

***Figure 36: Events that have mixed effects on confidence in infrastructures***

[Insert PowerPoint slide here]

# Figure 36: What factors have mixed effects on business user confidence in infrastructures (Users)?



**Figure 37: Impact of events on confidence in infrastructures  
(Q17 means and standard deviations)**

*(Excludes "Don't know" responses; base = 46 respondents)*

*(5 point rating scale where 1 = "strongly decrease," 2 = "slightly decrease," 3 = "neither," 4 = slightly increase and 5 = "strongly increase")*

	Mean	Standard Error of Mean	Standard Deviation	Valid N
Company reports five years of service with no outages	4.46	.09	.59	N=46
Major service outage due to a computer problem	1.85	.12	.84	N=46
Record of periodic outages but restores services rapidly	2.30	.18	1.23	N=46
Hacker unsuccessfully tries to break into computer system	4.11	.11	.77	N=46
Hacker successfully broke into computer system	1.58	.10	.69	N=45
Company is fined for violating a regulation	2.33	.14	.89	N=43
Voluntarily adheres to code for ethical business practices	3.96	.12	.84	N=46
Government enforces minimum standards for reliability	3.62	.14	.96	N=45
Has backup system in case of failures	4.52	.09	.59	N=46
Has no backup systems in case of failures	1.17	.06	.38	N=46
Has no adequate emergency response plan	1.13	.05	.34	N=45
Regularly rehearses emergency response plan	4.57	.11	.78	N=46
Outside auditors give clean bill of health for security/ reliability	4.22	.08	.51	N=46
Outside auditors find security and reliability problems	1.65	.10	.71	N=46
Company keeps customers informed about its operations	4.02	.09	.58	N=46
Company does not keep customers informed	1.93	.10	.71	N=46
Company identifies problems and announces plan to resolve them within one year	3.65	.13	.90	N=46
Company accused of hiding problems of security or reliability	1.33	.09	.60	N=46

**Figure 38: Impact of events on confidence in infrastructures  
(Q17 frequencies)**

(Excludes "Don't know" responses; base = 46 respondents)

		Strongly decrease	Slightly decrease	Neither	Slightly increase	Strongly increase	Don't know	Total
Company reports five years of service with no outages	N=	0	0	2	21	23	0	46
	%	0%	0%	4%	46%	50%	0%	100%
Major service outage due to a computer problem	N=	16	24	4	1	1	0	46
	%	35%	52%	9%	2%	2%	0%	100%
Record of periodic outages but restores services rapidly	N=	15	14	7	8	2	0	46
	%	33%	30%	15%	17%	4%	0%	100%
Hacker unsuccessfully tries to break into computer system	N=	0	2	5	25	14	0	46
	%	0%	4%	11%	54%	30%	0%	100%
Hacker successfully broke into computer system	N=	23	19	2	1	0	1	46
	%	50%	41%	4%	2%	0%	2%	100%
Company is fined for violating a regulation	N=	7	19	14	2	1	3	46
	%	15%	41%	30%	4%	2%	7%	100%
Voluntarily adheres to code for ethical business practices	N=	1	0	11	22	12	0	46
	%	2%	0%	24%	48%	26%	0%	100%
Government enforces minimum standards for reliability	N=	1	5	11	21	7	1	46
	%	2%	11%	24%	46%	15%	2%	100%
Has backup system in case of failures	N=	0	0	2	18	26	0	46
	%	0%	0%	4%	39%	57%	0%	100%
Has no backup systems in case of failures	N=	38	8	0	0	0	0	46
	%	83%	17%	0%	0%	0%	0%	100%
Has no adequate emergency response plan	N=	39	6	0	0	0	1	46
	%	85%	13%	0%	0%	0%	2%	100%
Regularly rehearses emergency response plan	N=	1	0	2	12	31	0	46
	%	2%	0%	4%	26%	67%	0%	100%
Outside auditors give clean bill of health for security/ reliability	N=	0	0	2	32	12	0	46
	%	0%	0%	4%	70%	26%	0%	100%
Outside auditors find security and reliability problems	N=	20	24	0	2	0	0	46
	%	43%	52%	0%	4%	0%	0%	100%
Company keeps customers informed about its operations	N=	0	0	7	31	8	0	46
	%	0%	0%	15%	67%	17%	0%	100%
Company does not keep customers informed	N=	13	23	10	0	0	0	46
	%	28%	50%	22%	0%	0%	0%	100%
Identifies problems & announces plan to resolve within year	N=	0	8	5	28	5	0	46
	%	0%	17%	11%	61%	11%	0%	100%
Company accused of hiding problems of security or reliability	N=	33	12	0	1	0	0	46
	%	72%	26%	0%	2%	0%	0%	100%

## **Systems used to protect operations from infrastructure failures**

Overwhelmingly, electrical power backup was the most often cited system. Many of those uninterruptible power supply (UPS) systems are in place to support the computer back-up system.

*“Uninterruptible for critical facilities power supply (safety, computer, fire). Some back up gas and oil. Back up routes for telecommunication. Alternate couriers from transportation.” (Manufacturing)*

*“We have uninterruptible power supply. Computer centers. Generators with seven to ten days duration of power. Tapes backed up. Remote transmit ‘critical information’ (corporate customer financial information and updates). Firewalls for information security. Software packages. Virus protection all personal computers.” (Banking/National)*

*“All critical systems on UPS and Generators on network side - back up power and redundant network to critical location. Same with the phone switches - backup and redundant switches. Also a number of security and software products in place. CAU center and some of the firewall products.” (Manufacturing)*

*“Uninterruptible power supply for building, computer data base, gas reserves in Springfield.” (Publishing/Broadcasting)*

*“Uninterruptible computer power supply—test every Tuesday. Evacuation plans. We use volumes of water so that’s important to us, too.” (Manufacturing)*

*“Back up power supplies. Backed up computers. Could switch banks.” (Restaurant/hotel)*

*“In the power area—we have back up generators. In telecommunications we have multi-company carriers (AT&T, MCI) so we don’t have all of our eggs in one basket. We also have a disaster recovery site where we can move our computer system. We have multi-delivery services so we do not depend on one carrier.” (Publishing/Broadcasting)*

*“For power we use UPS (Uninterrupted Power Suppliers) and generators for computer system. We also have a “hot site.” If power is cut off to our computer center for a long period of time, we move to our back up site. We also have a lot of redundant connections at extra cost.” (Retail)*

*“Backup power suppliers; transportation—no backup system; telecommunications—wireless communication system. Redundancy most companies maintain from backups for our computers. I will add one—water is extremely critical particularly in Life Sciences here in the Southwest. In our manufacturing processes, chips for our phones. Water is a scarce resource. If we don’t get it from Los Angeles, we don’t get any. If I were a hacker and wanted to shut down an industry, the first thing I would do would be to cut off water supply.” (Manufacturing)*

*“For electric power, UPS – Uninterrupted Power Supplies. That’s batteries and generators. Don’t have anything for transportation or fuel reserves as far as I know.” (Manufacturing)*

*“UPS – Uninterrupted Power Source. Virus protection and firewalls for computers. As far as transportation, we have contracts with alternate suppliers. Banking – extended lines of credit.” (Consumer products)*

*“Power back-up. UPS and generators to both of our data centers. That would work for a period of time. Second data center. Serves as recovery facility, and we back up our core systems to that recovery center. Terrorist or sabotage. Have security system – guards and badge system. Also established firewalls and access to security data.” (Financial services)*

*“Back-up power systems. Tape data storage. Fire protection or vaulted storage.” (Technology)*

*“We have back-up power suppliers. We use diesel generators, so we would be able to function past the twelve-hour period if the electric system went down for longer periods. With telecommunications, they have redundancy systems in place.” (Banking/Regional)*

*“Electric – We have code self generators. Gas and oil – We have long-term contracts with companies in most of our plants and as mentioned before, the option to switch from natural gas to oil in some plants. Telecommunications – Contingency networks. Banks – We have no option. We depend on the banks in the Federal system. Transportation – Rail is an option in the wholesale area, but we are heavily dependent on trucks.” (Consumer products)*

*“UPS back-up for computers. Back-up stored off site. Have similar UPS on phone switches. We do have the capability to frame a relay network. Company in another place could replicate our data base. Example: In case of an earthquake, we could still function. A company in New York has our system.” (Technology)*

*“We have back up power supplies. We have a supply of raw materials. Telecom – we use multiple carriers but no redundancy systems. (Consumer products)*

*“UPS for computer network and telephone system. Network systems only, PC’s aren’t covered in power failure. Phone has back-up for eight to twelve hours. When you start adding back-up, battery power. There’s a limit because of cost. UPS strike opened our eyes. We now have additional vendors, off-site storage, back-up. If network crashed or disappears, the off-site system brings it back up.” (Technology)*

*We have back up for our electric computer systems. Power suppliers. Transportation out of our control. (Restaurants/Hotels)*

*“Back-up power –electric. Disaster recovery back-up site – computer. Redundancy – telecom. Mineral oil to fuel-oil product. Transportation – none.” (Manufacturing)*

Back-ups for telecommunications systems were mentioned frequently as well.

*“In the power area—we have back up generators. In telecommunications we have multi-company carriers (AT&T, MCI) so we don’t have all of our eggs in one basket. We also have a disaster recovery site where we can move our computer system. We have multi-delivery services so we do not depend on one carrier.” (Publishing/Broadcasting)*

*“Electric – We have code self generators. Gas and oil – We have long-term contracts with companies in most of our plants and as mentioned before, the option to switch from natural gas to oil in some plants. Telecommunications – Contingency networks. Banks – We have no option. We depend on the banks in the Federal system. Transportation – Rail is an option in the wholesale area, but we are heavily dependent on trucks.” (Consumer products)*

*“We have critical recovery plan in place. Electric – Redundancy supplier, back-up generators in certain areas, not in all. Gas and oil – Mutual redundancy sources. Recovery mode with regional people to help. Transportation – We are not directly responsible. The people we contract with deal mainly with issue. **Telecommunications – We have computer fault tolerance lines. Inter- and intra-state redundancy systems.** Banking and Finance – We have exchange agreements with several banks. If one fails, another picks up. We don’t stick to only one bank in the world.” (Technology)*

*“Telecom – we have double lines – designed that if everything goes out on one line, power turns around and comes back. We have multi service providers – AT&T is our different line. MCI & Sprint. Power – back-up diesel generators and we get power from two separate grids. Transportation – we have created our own transportation company. We have built-in redundancy.” (Technology)*

*“We have mobile data center. Telecommunications tech can be rerouted.”  
(Banking/National)*

*“Telecom – redundancy/different paths. Self-contained generators.  
Contracts with other providers (computer). Recovery plan. Muscle our way  
through it.” (Consumer products)*

Several respondents elaborated on all encompassing systems:

*“We have systems and plans for everything. Business continuation group to  
evaluate. Emergency repose team set up - drills - beepers for the team  
numbers. Operating center is backed up well; off sites have some electric back  
ups. Fuel and oil back ups as well. Virus scanners, firewalls, access cards for  
employees, cameras, guards, access codes/passwords. Structurally operations  
center is well designed. Computer rooms enhanced in new center which is  
being constructed.” (Financial services)*

*“Back up fuel supplies; computer and telecommunications tied into one -  
backups and disaster recovery program—software and procedure; no back up  
for electrical power—would transfer product to warehouse if critical;  
Trucking could contact other companies but two to three day lag.” (Retail)*

*“We have back up on everything.” (Banking/Regional)*

*“The normal back-ups. Back-up on disks. Store off-site. But we had our  
back-up site burn down, which really makes you stop and think. Limited  
access to computer room and thorough background checks of employees.  
Normal cut-off switches. Generators, things like that.” (Pharmaceuticals)*

*“Standard back-ups. Limited duration. Computer backed up with limited  
supply. Generator only for parts, not all of the company.” (Consumer  
products)*

*“Off-site. Hot site. Second computer facility. Energy back-up is diesel. We  
don’t use oil.” (Consumer products)*

*“Our corporation has emergency disaster processes in place designed to deal  
with all abnormal intrusion of services – all-inclusive.” (Local telephone)*

*“We have back-up systems and a manual gas generator. We have to take it  
outside to fire it up. We use UPS. For telephone, we have two major circuits  
and soon to have a third for Internet.” (Retail)*

*“We have mirrored systems for uninterrupted power supply. As to the  
Internet and Intranet, we have multiple carriers. As far as transportation,  
we have a lot of companies to service us. We do not rely on one company.  
And banking, we use multiple banks in multiple locations.” (Direct  
marketing)*

## Perceptions of the transparency of infrastructure owners about reliability

Survey participants were divided about whether infrastructure owners keep the companies informed about the reliability and security of the infrastructures, and what the owners are doing to assure system reliability and integrity.

- Many respondents feel that owners are indeed open and clear about system reliability and dependability.

*“They do a fair job. We have very good communication with the operators especially on the security side.” (Banking/Regional)*

*“Yes, we have internal briefings on a regular basis.” (Technology)*

*“Some – Telecommunications does a good job. Power systems are beginning to attempt expanded communications. This is true also for the financial industry. Oil and gas seem to be falling behind in this area.” (Local telephone)*

- However, many others feel that infrastructure owners are not sufficiently open about their operations.

*“No, because I really don’t know what level of security they provide. They have not actively given us that information.” (Technology)*

*“Not at all; [we have] no real dialogue because [there is] no one owner. Went through two agencies to find problem.” (Manufacturing)*

Unfortunately, over one-half of the respondents felt they are not informed about back-up system vulnerabilities.

*“No. They don’t have to address it. The public takes it for granted.” (Manufacturing)*

*“Generally no—under-informed in general. From our business viewpoint that deals with encryption and the building blocks of the new technology being on the front line. I don’t know how they could possibly tell us how vulnerable they are.” (Manufacturing)*



## Appendix: Questionnaire

---

### INFRASTRUCTURE USERS SURVEY FHR 201992

Hello. This is \_\_\_\_\_ from Fleishman-Hillard Research. We are calling on behalf of the President's Commission on Critical Infrastructure Protection. This commission was formed to develop a strategy for protecting and assuring the continued operation of the nation's critical infrastructures such as telecommunications systems, computer networks, energy supply, air and ground transportation, and banking and financial systems. (IF NECESSARY, OFFER TO FAX MORE INFORMATION.)

To help with this task, we are interviewing senior executives at a range of companies. Your viewpoints would be extremely valuable to the commission. This interview is confidential and your comments will not be associated with you or your organization. Would now be a good time to talk? (IF ASKED, This will take about 15 minutes or so).

- 1 YES -- CONTINUE
- 2 NO – SCHEDULE A TIME TO CALL BACK

For this study, we are focusing on threats that include the following:

- physical threats from criminals, company employees, or others who want to harm the organization's ability to deliver its services,
- failures of key systems due to human error, or technological failure,
- terrorism, and
- cyber-threats, for example, electronic or computer-based threats to the information or communications systems on which we all depend.

## CONFIDENCE

1. How confident are you in the ability of each of the following systems to provide dependable, reliable services to your company? Please use a 10-point scale where one means not at all confident and ten means extremely confident.

	Not at all					Extremely					Don't know
Electric power system?	1	2	3	4	5	6	7	8	9	10	11
Gas and oil production, storage and transportation?	1	2	3	4	5	6	7	8	9	10	11
Telecommunications?	1	2	3	4	5	6	7	8	9	10	11
Banking and finance?	1	2	3	4	5	6	7	8	9	10	11
Transportation, including airlines, railroads and trucking?	1	2	3	4	5	6	7	8	9	10	11

## THREATS

2. In your opinion, how vulnerable is the electric power system to the following threats? Please use a 10-point scale where one means not at all vulnerable and ten means extremely vulnerable.

	Not at all					Extremely					Don't know
Technical failures or human errors?	1	2	3	4	5	6	7	8	9	10	11
Physical damage due to terrorists?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems due to cyber terrorism, including computer hackers or viruses?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems by a disgruntled employee?	1	2	3	4	5	6	7	8	9	10	11

3. In your opinion, how vulnerable is gas and oil production, storage and transportation to the following threats? Please use a 10-point scale where one means not at all vulnerable and ten means extremely vulnerable.

	<b>Not at all</b>					<b>Extremely</b>					<b>Don't know</b>
Technical failures or human errors?	1	2	3	4	5	6	7	8	9	10	11
Physical damage due to terrorists?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems due to cyber terrorism, including computer hackers or viruses?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems by a disgruntled employee?	1	2	3	4	5	6	7	8	9	10	11

4. In your opinion, how vulnerable is the telecommunications system to the following threats? Please use a 10-point scale where one means not at all vulnerable and ten means extremely vulnerable.

	<b>Not at all</b>					<b>Extremely</b>					<b>Don't know</b>
Technical failures or human errors?	1	2	3	4	5	6	7	8	9	10	11
Physical damage due to terrorists?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems due to cyber terrorism, including computer hackers or viruses?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems by a disgruntled employee?	1	2	3	4	5	6	7	8	9	10	11

5. In your opinion, how vulnerable is the banking and finance system to the following threats? Please use a 10-point scale where one means not at all vulnerable and ten means extremely vulnerable.

	<b>Not at all</b>					<b>Extremely</b>					<b>Don't know</b>
Technical failures or human errors?	1	2	3	4	5	6	7	8	9	10	11
Physical damage due to terrorists?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems due to cyber terrorism, including computer hackers or viruses?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems by a disgruntled employee?	1	2	3	4	5	6	7	8	9	10	11

6. In your opinion, how vulnerable is the transportation system to the following threats? Please use a 10-point scale where one means not at all vulnerable and ten means extremely vulnerable.

	<b>Not at all</b>					<b>Extremely</b>					<b>Don't know</b>
Technical failures or human errors?	1	2	3	4	5	6	7	8	9	10	11
Physical damage due to terrorists?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems due to cyber terrorism, including computer hackers or viruses?	1	2	3	4	5	6	7	8	9	10	11
Disruption of its computer and telecommunications systems by a disgruntled employee?	1	2	3	4	5	6	7	8	9	10	11

**RELIANCE**

7. On a scale of one to ten where one means not at all critical and ten means extremely critical, how critical is each of these systems to your company's operations?

	<b>Not at all</b>					<b>Extremely</b>					<b>Don't know</b>
	1	2	3	4	5	6	7	8	9	10	11
Electric power system	1	2	3	4	5	6	7	8	9	10	11
Gas and oil production, storage and transportation	1	2	3	4	5	6	7	8	9	10	11
Telecommunications	1	2	3	4	5	6	7	8	9	10	11
Banking and finance	1	2	3	4	5	6	7	8	9	10	11
Transportation, including airlines, railroads and trucking	1	2	3	4	5	6	7	8	9	10	11

8. Which one organization is most critical to your company's operation?

9. If the following system failed, for what length of time could your company continue to function before a crisis situation developed? Please describe the effects of such a failure.

Electric power system (RECORD VERBATIM)

LENGTH OF TIME:

EFFECTS:

Gas and oil production, storage and transportation (RECORD VERBATIM)

LENGTH OF TIME:

EFFECTS:

Telecommunications (RECORD VERBATIM)

LENGTH OF TIME:

EFFECTS:

Banking and finance (RECORD VERBATIM)

LENGTH OF TIME:

EFFECTS:

Transportation, including airlines, railroads and trucking (RECORD VERBATIM)

LENGTH OF TIME:

EFFECTS:

10. Thinking about the potential failure of any of the systems we have been talking about, what is your single biggest concern for the short term?
11. For the long term?

### **EXPERIENCE**

12. Has your company experienced a failure or service disruption of any of these critical infrastructures during the past few years?
  - 1 YES – ASK Q. 13
  - 2 NO
  - 3 DON'T KNOW
13. How did this affect your company?
14. What kinds of systems does your company have in place to protect your operations from the failure of each of these infrastructures? Please include

anything from backup power supplies to computer backups and systems to protect the security of your computers.

**TRANSPARENCY**

- 15. Do you feel that the owners or operators of these systems keep you adequately informed about their operations, and the level of security or reliability that they provide?
  
- 16. Do you feel that they are open and honest about the potential for a system failure? Please explain.

**ELASTICITY QUESTIONS**

- 17. Now I would like you to think specifically about **(MOST CRITICAL INFRASTRUCTURE FROM Q.8)**. I am going to read a list of possible events. For each event, please tell me whether this would strongly increase your confidence in that organization, slightly increase your confidence, slightly decrease, or strongly decrease your confidence in that organization.

ROTATE QUESTIONS	Strongly Increase	Slightly Increase	Neither	Slightly Decrease	Strongly Decrease	Don't Know
<b>RELIABILITY</b>						
<b>The company reports five years of service with no outages (CHI)</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>6</b>
<b>Has a major service outage due to a computer problem (CD)</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>6</b>
<b>Has a record of periodic service outages but restores services rapidly (CHI)</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>6</b>
<b>A hacker tried to break into the company's computer systems but was not successful (CHI)</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>6</b>
<b>A hacker successfully broke into the company's computer systems (CD)</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>6</b>

	Strongly Increase	Slightly Increase	Neither	Slightly Decrease	Strongly Decrease	Don't Know
<b>REGULATION/ETHICS CODES</b>						
<b>The company is fined for violating a regulation (CD)</b>	5	4	3	2	1	6
<b>The company voluntarily adheres to an industry code for ethical business practices (CHI)</b>	5	4	3	2	1	6
<b>The government enforces minimum standards for reliability (CHI)</b>	5	4	3	2	1	6
<b>INTERNAL SUPERVISION/SECURITY</b>						
<b>Has backup systems in case of failures (CHI)</b>	5	4	3	2	1	6
<b>Has no backup systems in case of failures (CD)</b>	5	4	3	2	1	6
<b>Has no adequate emergency response plan (CD)</b>	5	4	3	2	1	6
<b>Regularly rehearses its emergency response plan (CHI)</b>	5	4	3	2	1	6
<b>THIRD PARTY AUDITS &amp; STANDARDS</b>						
<b>Outside auditors give the company a clean bill of health for security and reliability (CHI)</b>	5	4	3	2	1	6
<b>Outside auditors find security and reliability problems (CD)</b>	5	4	3	2	1	6

	Strongly Increase	Slightly Increase	Neither	Slightly Decrease	Strongly Decrease	Don't Know
<b>TRANSPARENCY</b>						
<b>The company keeps you informed about its operations (CHI)</b>	5	4	3	2	1	6
<b>The company does not keep you informed about its operations (CHI)</b>	5	4	3	2	1	6
<b>The company identifies problems and announces plans to resolve them within one year (CHI)</b>	5	4	3	2	1	6
<b>The company is accused of hiding problems of security or reliability (CD)</b>	5	4	3	2	1	6

Those are all my questions. Are there any additional comments you'd like to make?

Thank you for participating.

RESPONDENT'S NAME: \_\_\_\_\_

TITLE: \_\_\_\_\_

COMPANY NAME: \_\_\_\_\_

PHONE NUMBER: \_\_\_\_\_

INTERVIEWER: \_\_\_\_\_ DATE: \_\_\_\_\_ LENGTH: \_\_\_\_\_ MINUTES

# INFRASTRUCTURE OWNERS/OPERATORS SURVEY

## FHR 201992

Hello. This is \_\_\_\_\_ from Fleishman-Hillard Research calling on behalf of the President’s Commission on Critical Infrastructure Protection. This commission was formed to develop a strategy for protecting and assuring the continued operation of the nation’s critical infrastructures such as telecommunications systems, computer networks, energy supply, air and ground transportation, and banking and financial systems. (IF NECESSARY, OFFER TO FAX MORE INFORMATION.) We would like to talk to you as an operator of an infrastructure. This interview is confidential and your comments will not be associated with you or your organization. Would now be a good time to talk? (IF ASKED, This will take about 15 minutes).

- 1 YES -- CONTINUE
- 2 NO – SCHEDULE A TIME TO CALL BACK

### THREATS

1. How vulnerable are your company’s services to the following threats? Please use a 10-point scale where one means not at all vulnerable and ten means extremely vulnerable. **(ROTATE ORDER)**

	Not at all					Extremely					Don’t Know
	1	2	3	4	5	6	7	8	9	10	11
Technical failures or human errors?	1	2	3	4	5	6	7	8	9	10	11
Physical damage due to terrorists?	1	2	3	4	5	6	7	8	9	10	11
Disruption of your computer and telecommunications systems due to cyber terrorism, including computer hackers or viruses?	1	2	3	4	5	6	7	8	9	10	11
Disruption of your computer and telecommunications systems by a disgruntled employee?	1	2	3	4	5	6	7	8	9	10	11

2. What is your company doing to protect itself from the following types of threats:

2.1 Technical failures and human errors?

2.2 Physical damage due to terrorists?

2.3 Disruption of your computer and telecommunications systems due to cyber terrorism?

2.4 Disruption of your computer and telecommunications systems by a disgruntled employee?

**PUBLIC CONFIDENCE**

3. On a 10-point scale where one means not at all confident and ten means extremely confident,

	<b>Not at all</b>					<b>Extremely</b>					<b>Don't Know</b>
	1	2	3	4	5	6	7	8	9	10	11
How confident would you say your business customers are in the ability of your company to provide reliable service?											
On the same scale, how confident are your non-business customers?	1	1	1	1	1	1	1	1	1	1	1

4. What do you consider to be the major threats to public confidence in your industry at this time? (RECORD VERBATIM.)

5. What might they be in two years? (RECORD VERBATIM.)

6. Has your organization experienced any significant events that might have damaged public confidence?

1 YES – ASK Q. 7.

2 NO

KNOW/REFUSED

7. What were these events? What was the impact?

8. All industries experience periodic service outages that may affect public confidence. What steps might your company take to reassure the public after an outage has occurred?

No Q. 9.

**ELASTICITY QUESTIONS**

10. I am going to read a list of possible events. For each event, please tell me whether this would strongly increase public confidence in your organization, slightly increase public confidence, slightly decrease, or strongly decrease public confidence in your organization.

**(ROTATE ORDER)**

	<b>Strongly Increase</b>	<b>Slightly Increase</b>	<b>Neither</b>	<b>Slightly Decrease</b>	<b>Strongly Decrease</b>	<b>Don't Know</b>
<b>RELIABILITY</b>						
Your company reports five years of service with no outages (CI)	5	4	3	2	1	6
Has a major service outage due to a computer problem (CD)	5	4	3	2	1	6
Has a record of periodic service outages but restores services rapidly (CI)	5	4	3	2	1	6
A hacker tried to break into your computer systems but was not successful (CI)	5	4	3	2	1	6
A hacker successfully broke into your computer systems (CD)	5	4	3	2	1	6

	<b>Strongly Increase</b>	<b>Slightly Increase</b>	<b>Neither</b>	<b>Slightly Decrease</b>	<b>Strongly Decrease</b>	<b>Don't Know</b>
<b>REGULATION/ETHICS CODES</b>						
Your company is fined for violating a regulation (CD)	5	4	3	2	1	6
Voluntarily adheres to an industry code for ethical business practices (CI)	5	4	3	2	1	6
The government enforces minimum standards for reliability (CI)	5	4	3	2	1	6
<b>INTERNAL SUPERVISION/ SECURITY</b>						
Has backup systems in case of failures (CI)	5	4	3	2	1	6
Has no backup systems in case of failures (CD)	5	4	3	2	1	6
Has no adequate emergency response plan (CD)	5	4	3	2	1	6
Regularly rehearses its emergency response plan (CI)	5	4	3	2	1	6
<b>THIRD PARTY AUDITS &amp; STANDARDS</b>						
Outside auditors give your company a clean bill of health for security and reliability (CI)	5	4	3	2	1	6
Outside auditors find security and reliability problems (CD)	5	4	3	2	1	6
<b>TRANSPARENCY</b>						
Your company keeps the community and customers informed about its operations (CI)	5	4	3	2	1	6
Your company does not keep the community and customers informed about its operations (CI)	5	4	3	2	1	6
Your company identifies problems and announces plans to resolve them within one year (CI)	5	4	3	2	1	6
Your company is accused of hiding problems of security or reliability (CD)	5	4	3	2	1	6

Those are all my questions. Are there any additional comments you'd like to make?

Thank you for participating.

RESPONDENT'S NAME: \_\_\_\_\_

TITLE: \_\_\_\_\_

COMPANY  
NAME: \_\_\_\_\_

PHONE  
NUMBER: \_\_\_\_\_

INTERVIEWER: \_\_\_\_\_ DATE: \_\_\_\_\_

LENGTH: \_\_\_\_\_ MINUTES