

PUBLIC CONFIDENCE

Report of the
President's Commission
on Critical Infrastructure Protection

1997



ACKNOWLEDGMENTS

The Commission gratefully acknowledges the singular leadership and important contributions to this report made by Commissioner Mary Culnan, and thanks her for increasing our understanding of public confidence issues. The Commission also thanks the firm of Fleishman-Hillard Research for their work in preparing the survey instruments referenced herein, polling the respondents, and conducting the relevant analyses.

Public Confidence

“Well, the planes run out there, and the phones work out there, and the E-mail works out there, so we’ll be all right.”

Response of President Clinton when asked how he felt about his daughter Chelsea choosing a college in California, New York Times, May 1, 1996.

Introduction

Public confidence affects the bottom line for both the government and business. In the private sector, public confidence is one basis for attracting and retaining customers, while in the public sector, it is the basis of political legitimacy. For both, it is essential to remaining in business. For critical infrastructures, public confidence means that infrastructures perform in accordance with expectations, and that infrastructure owners and operators can be trusted to act in the best interests of their customers¹. As the quotation from President Clinton illustrates, Americans today typically have a very high level of confidence in our critical infrastructures. The fact that our infrastructures provide consistently reliable service is also a source of competitive advantage for the country in the global economy.

This paper will address two issues. First, it will describe how public confidence is created and maintained. Second, it will describe the results of a research project which surveyed the confidence that both infrastructure owners/operators and their business customers have in critical infrastructures.

¹ See Summary of Academic Workshop on Public Confidence, President’s Commission on Critical Infrastructure Protection, May 30, 1997.

Creation and Maintenance of Public Confidence

Public confidence reflects the trust that a user has in the infrastructure. There are four factors which influence the creation and maintenance of public confidence and lead the user to believe that the infrastructure owner can be trusted: 1) transparency including openness about operations, and accountability, 2) reliability and competence including the ability to perform consistently at an appropriate level, 3) fairness or an absence of bias, and 4) integrity.

Trust reflects a willingness to assume the risks of participating in a relationship with an infrastructure owner where the user must depend on strangers to act on their behalf. Once a user has an ongoing relationship with an infrastructure owner, both trust and confidence accrue from the customer's first-hand experiences. When a user initiates a customer relationship with an infrastructure, surrogates or intermediaries that can substitute for this first-hand knowledge are needed to signal to the user that the infrastructure owner can be trusted, absent first-hand experience. These substitute measures include standards, audits, insurance, laws and regulations, ethical codes, inspection, compliance officers and oversight². These surrogates and intermediaries also serve to reinforce the trust that accumulates as a result of experience. The figure below illustrates how confidence is created and maintained.

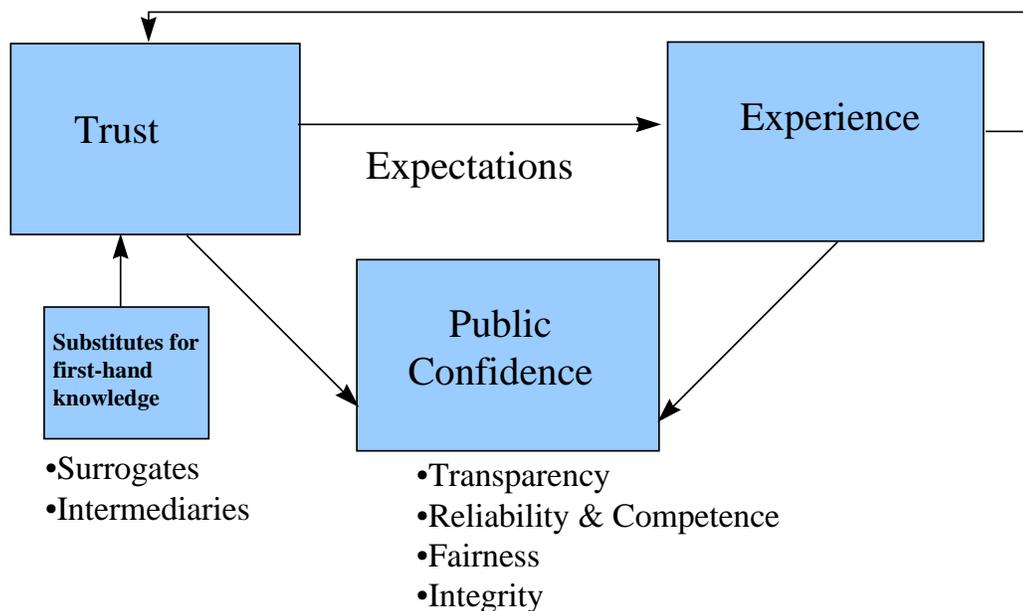


Figure 1: Creation & Maintenance of Public Confidence

² See Susan P. Shapiro, "The Social Control of Impersonal Trust," *American Journal of Sociology*, 93, 3, 623-58, Nov. 1987.

Even though the majority of critical infrastructures are owned and operated by the private sector, government has a legitimate, albeit limited role to play in the creation and maintenance of public confidence. Government should assume primary responsibility for assuring that an infrastructure owner or operator can be trusted where it is difficult for customers to establish and monitor trust, and where the service is a public good. In the majority of other cases, market forces should prevail since in these instances, both information and alternatives should be available to promote informed choice by both business and consumer customers.

Public Confidence as Viewed by Infrastructure Owners/Operators and Their Business Customers

Methodology

The Commission surveyed both infrastructure owners and operators and business users to understand how these two groups view the ability of the infrastructures to withstand physical and cyber threats, and the procedures owners and operators can implement to protect their operations. We also measured the “elasticity of confidence,” the extent to which various factors cited above such as transparency and reliability or events such as a hacker break-in are perceived by these two audiences as creating or diminishing confidence. While there was overlap between the two surveys, the questionnaires were tailored for the respective audiences. The research was conducted for the Commission by Fleishman-Hillard Research³.

Telephone interviews were conducted with 100 senior executives or senior managers with operational responsibilities from infrastructure owners/operators and users. The interviews were evenly divided between the owners/operators and the users. Infrastructure owners and operators represented telecommunications, banking and finance, energy generation, transmission and distribution, and transportation. Infrastructure users represented private sector companies across a range of industries including retail banking, consumer products, healthcare, manufacturing, technology, and retail and hotel/restaurants. While infrastructure owners/operators are in fact also users of other infrastructures, the owners were only asked to provide answers from the perspective of an owner/operator.

³ See final report: Opinion Survey of Infrastructure Owners and Users, conducted by Fleishman-Hillard Research for the President’s Commission on Critical Infrastructure Protection, October 1997.

Survey of Infrastructure Owners & Operators: Key Findings

Perceived infrastructure vulnerability

Overall, owners and operators do not feel that their respective infrastructures are very vulnerable to any of the threats included in the survey, 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 to terrorism have distributed or multiple facilities and/or highly visible facilities with public access such as firms in the transportation or vital human services sectors.

Perceptions of customer confidence in the infrastructures

Infrastructure owners and operators 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.

Initiatives to provide infrastructure protection

Infrastructure owners and operators 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 mitigate the damages resulting from a terrorist or cyber-terrorist attack. These 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 and operators 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 and operators feel that three categories of events have actually reduced public confidence in their infrastructures: 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 and operators 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; and
- Rapidly restore service after a service interruption.

Survey of Infrastructure Users: Key Findings

Most critical infrastructures to company operations

Users were asked how critical each of the five infrastructure sectors is to their operations. Business executives resoundingly feel that telecommunications and electric power are the most critical infrastructures to their company operations, followed by banking and 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 and 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 are 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 by users 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 on users

- *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 Public Confidence

The elasticity of public confidence refers to its resiliency in the face of events that either increase or diminish confidence. Both owners and operators and the business users were asked to what extent eighteen different factors or events either increased or decreased their confidence in infrastructures. Questions covered five categories: reliability, regulations or codes of ethics, internal supervision and security, third party audits and standards, and transparency of operations. Owners and operators were asked to respond for their own organization while users were asked to respond for their most critical infrastructure.

Tables 1 and 2⁴ reflect the rankings of the factors and events that either increase or decrease confidence respectively for the owners/operators and the users. It is interesting to note that for both categories, while the rankings differ slightly, the owners/operators and the users identified the same items as increasing and decreasing confidence.

Owners and Operators

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.

Users

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 and operators feel tend to increase public confidence.

- **Contingency or emergency planning and preparation** lead all other actions in increasing business confidence in infrastructures among business users 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 among business users. We can speculate that proven reliability is a

⁴ See page 12 and 13.

- cost-of-entry for an infrastructure provider, but that the ability to handle crises and system failures differentiates among infrastructure owners and operators.

For business users, learning that an infrastructure withstood an attack by a computer hacker also increases confidence. For infrastructure owners and operators, this type of event received more mixed ratings.

- **Transparency** of company operations and planning is viewed as critical. The users feel that infrastructure owners and operators 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.

Public Confidence and the Public

The Commission was unable to survey the general public about their confidence in infrastructures⁵. However, prior research by Slovic⁶ for the nuclear power industry suggests that transparency, emergency planning, and being responsive to problems – many of the same factors that build confidence for business users – are applicable for the general public.

The Slovic paper, however, reflects only one aspect of public confidence: how the public perceives a risk in their community and what steps the infrastructure operator, here the operator of a nuclear power plant, can take to communicate to the public that the risks the facility presents to the local community are being appropriately managed. The Slovic paper does not address public confidence in infrastructures from the perspective of the consumer as a customer of the infrastructure. Business users may view confidence through a different lens than consumers. For example, business users viewed an unsuccessful hacker attack as confidence increasing. It is not clear how such an event, particularly if it received a large amount of media attention, would be viewed by consumers with a low level of computer literacy. Public opinion research is clearly needed to fully understand the drivers of consumer confidence in critical infrastructures.

⁵ The Office of Management & Budget stated that the survey did not meet the requirements of the Paperwork Reduction Act.

⁶ Paul Slovic, Perceived Risk, Trust and Democracy, *Risk Analysis*, Vol 13, No. 6, p. 675-682, 1993.

Conclusion

Both infrastructure owners/operators and their business customers have a great deal of confidence in the ability of the critical infrastructures to deliver reliable service. The elasticity data suggest that is a result of owners/operators following industry best practices and by so doing, signal to their business customers that they can be trusted. It is interesting to note that the one confidence-increasing factor involving government (government enforcing minimum standards for reliability) was rated last by both owners/operators and users. This suggests that in today's environment, market forces are working and the Commission does not need to recommend any government action at the present time.

This picture could change slightly with deregulation of both energy and telecommunications where new players will enter the market and the trusted environment that exists today may no longer be taken for granted. It may be necessary to develop new means for ensuring that new players do no harm to the infrastructures and that customers have the information they need to make informed choices while ensuring a level playing field for all competitors. In particular, consumers may need the government to take steps to ensure that they have the information they need to make choices that will lead to reliable service at a competitive price. Making reliability data on network outages public is one example of the type information that could serve this purpose. However, even the changing competitive environment calls for very limited action on the Government's part absent a failure of the market.

Should some unforeseen future event result in a decline in public confidence in one or more infrastructures that cannot be addressed by the market, the existing procedures that currently create confidence will need to be augmented. For example, in Table 2, a company identifying problems and announcing plans to resolve them within a fixed time period does little to increase public confidence.

The Slovic article cited previously suggests that the best way to accomplish this is through greater transparency and control provided by appointing an outside advisory board that can provide independent oversight for the infrastructure in question. For the nuclear power plant example in Slovic's article, the one factor that increased public trust the most was a local board with authority to close the plant. Another example of the use of transparency and oversight to rebuild trust and confidence in a critical system when current procedures have failed is President Clinton's proposal to create an independent Citizen's Review Panel to field taxpayer complaints about the Internal Revenue Service in the wake of the massive abuses disclosed at the recent

Senate oversight hearings⁷. Similar steps should be considered if warranted by circumstances for critical infrastructures.

Finally, the research assessed the attitudes of the owners and operators from the perspective of owners of independent firms. It does not provide insights about interdependencies: either from the perspective of the owner/operator as user whose operations are dependent upon other infrastructures, or to assess the attitudes of the owner/operator concerning the role of its firm in the functioning of the entire infrastructure. Future research should address both of these issues.

⁷ Clay Chandler and Albert B. Crenshaw, "Clinton to Propose Board to Act as IRS Watchdog," The Washington Post, October 3, 1997, p. A1.

Table 1
Factors that Increase Confidence in Infrastructures (Mean)

<u>Owners</u>	<u>Business Users</u>
1. Company reports five years of service with no outages (4.70)	1. Regularly rehearses emergency response plan (4.63)
2. Company keeps community informed about its operations (4.41)	2.5 Company reports five years of service with no outages (4.50)
3. Has backup system in case of failures (4.29)	2.5 Has backup system in case of failures (4.50)
4. Outside auditors give clean bill of health for security/reliability (4.23)	4. Outside auditors give clean bill of health for security/reliability (4.22)
5. Voluntarily adheres to code for ethical business practices (4.08)	5. Hacker unsuccessfully tries to break into computer system (4.13)
6. Regularly rehearses its emergency response plan (4.04)	6.5 Voluntarily adheres to ethical code for business practices (4.03)
7. Hacker unsuccessfully tries to break into computer system (3.65)	6.5 Company keeps customers informed about its operations (4.03)
8. Company identifies problems and announces plans to resolve them within one year (3.47)	8. Company identifies problems and announces plans to resolve them within one year (3.65)
9. Government enforces minimum standards for reliability (3.20)	9. Government enforces minimum standards for reliability (3.62)

Rankings based on mean for item where 1=strongly decrease confidence, 2=slightly decrease confidence, 3= neither, 4=slightly increase confidence, and 5=strongly increase confidence.

Table 2
Factors that Decrease Confidence in Infrastructures (Mean)

<u>Owners</u>	<u>Business Users</u>
1. Has no backup systems in case of failures (1.38)	1. Has no adequate emergency response plan (1.13)
2. Company accused of hiding problems of security or reliability (1.41)	2. Has no backup systems in case of failures (1.18)
3. Has no adequate emergency response plan (1.46)	3. Company accused of hiding problems of security or reliability (1.30)
4. Hacker successfully broke into computer system (1.68)	4. Hacker successfully broke into computer system (1.54)
5. Outside auditors find security and reliability problems (1.77)	5. Outside auditors find security and reliability problems (1.68)
6. Major service outage due to a computer problem (1.80)	6. Major service outage due to a computer problem (1.85)
7. Company does not keep community informed about its operations (1.89)	7. Company does not keep customers informed (1.88)
8. Company is fined for violating a regulation (1.95)	8. Record of periodic outages but restores services rapidly (2.23)
9. Record of periodic outages but restores services rapidly (2.80)	9. Company is fined for violating a regulation (2.32)

Rankings based on mean for item where 1=strongly decrease confidence, 2=slightly decrease confidence, 3= neither, 4=slightly increase confidence, and 5=strongly increase confidence.