Protecting Information Infrastructures

Rich Pethia

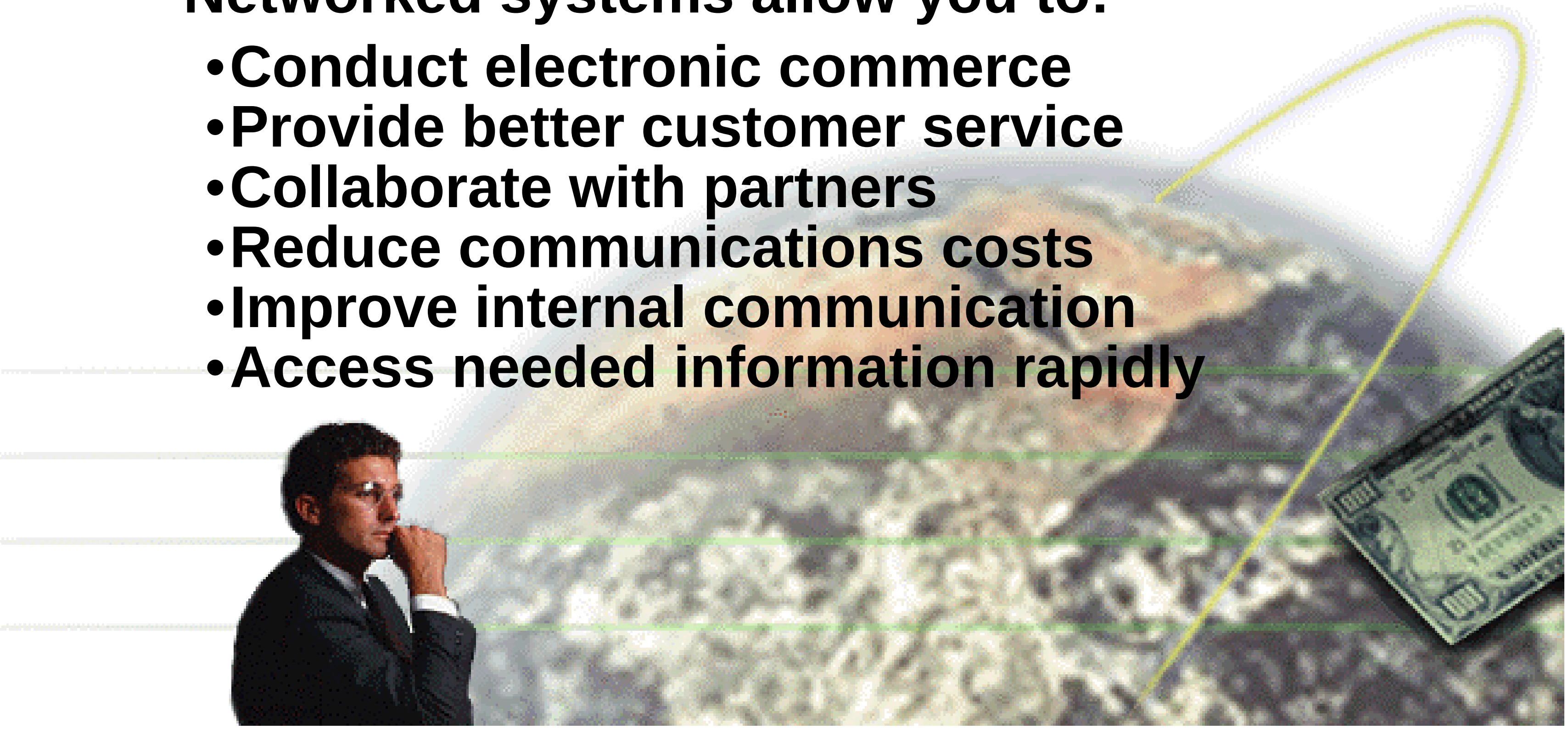
**Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213**

**This work is sponsored by the
U.S. Department of defense.**

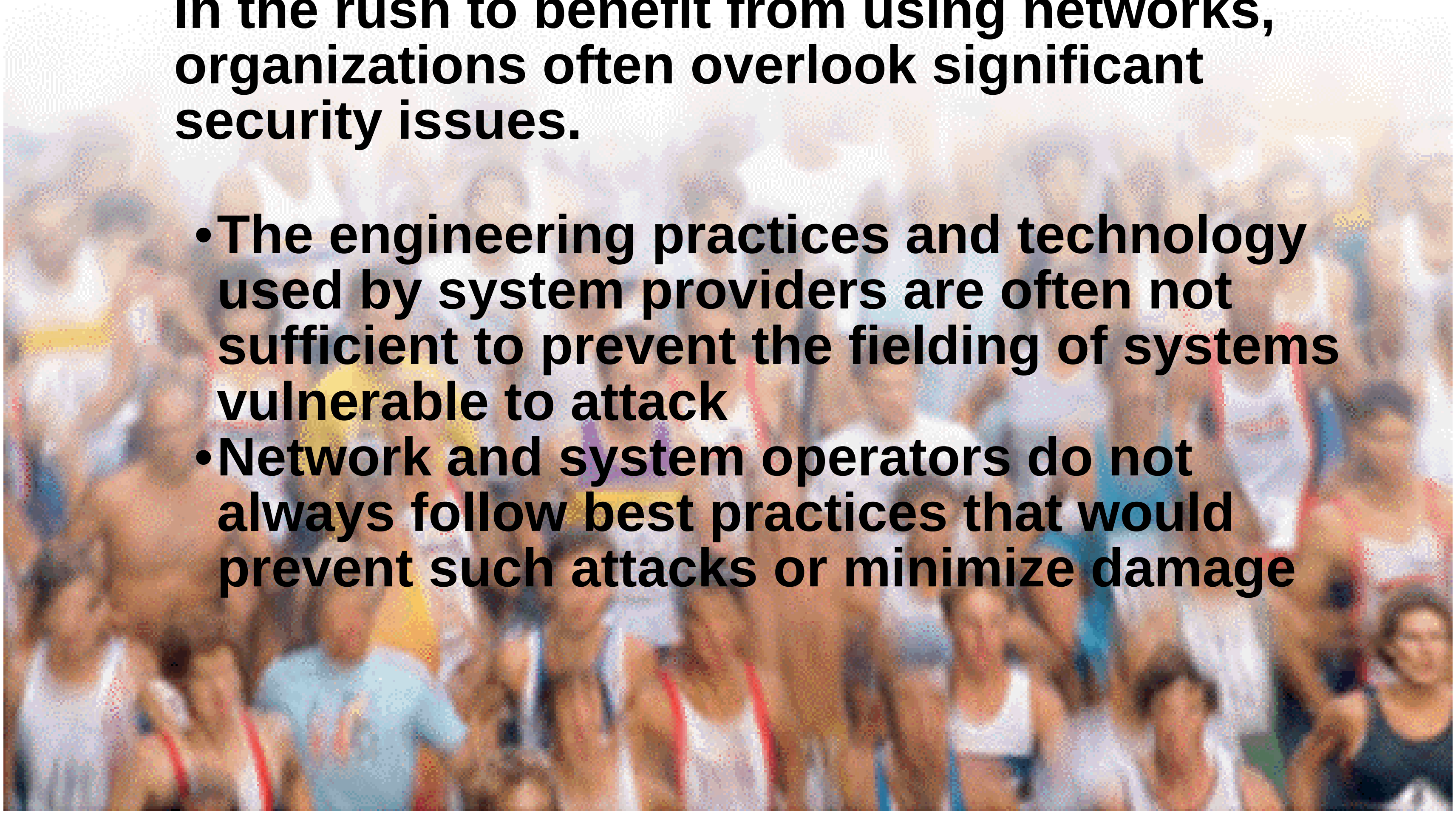
Networks Are Indispensable to Your Business

Networked systems allow you to:

- **Conduct electronic commerce**
- **Provide better customer service**
- **Collaborate with partners**
- **Reduce communications costs**
- **Improve internal communication**
- **Access needed information rapidly**



The Problem



In the rush to benefit from using networks, organizations often overlook significant security issues.

- **The engineering practices and technology used by system providers are often not sufficient to prevent the fielding of systems vulnerable to attack**
- **Network and system operators do not always follow best practices that would prevent such attacks or minimize damage**

The Risks

While computer networks revolutionize the way you do business, the risks computer networks introduce can be fatal to a business.

Network attacks lead to lost:

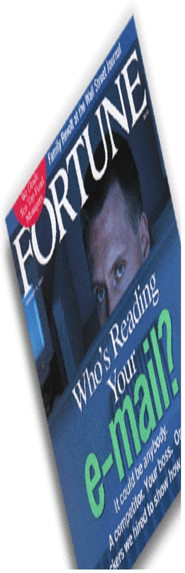
- **Money**
- **Time**
- **Products**
- **Reputation**
- **Lives**
- **Sensitive information**

Family Revolt at the Wall Street Journal
FORTUNE
We Grade Ten Top Fund Managers
Who's Reading Your e-mail?
It could be anybody.
A competitor. Your boss. Or
ckers we hired to show how

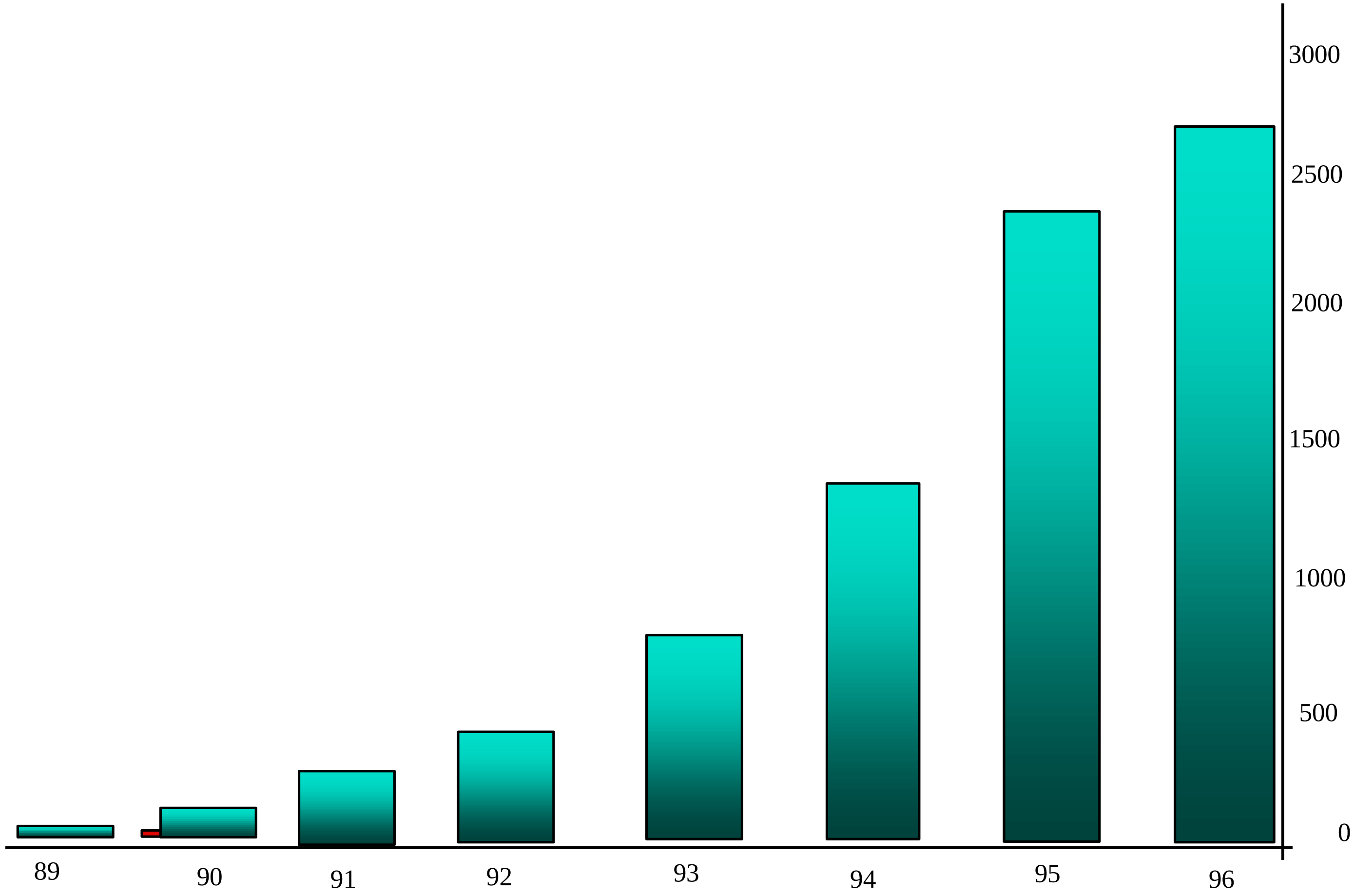
Recent examples

Increasing damage from attacks

- **high technology bank robbery**
- **loss of intellectual property - $2M in one case**
- **extensive compromise of operational systems - 15,000 hour recovery operation in one case**
- **medical records tampering**
  - **altering results of diagnostic tests**
  - **compromising the integrity of CAT scan data**
- **extortion - demanding payments to avoid operational problems**



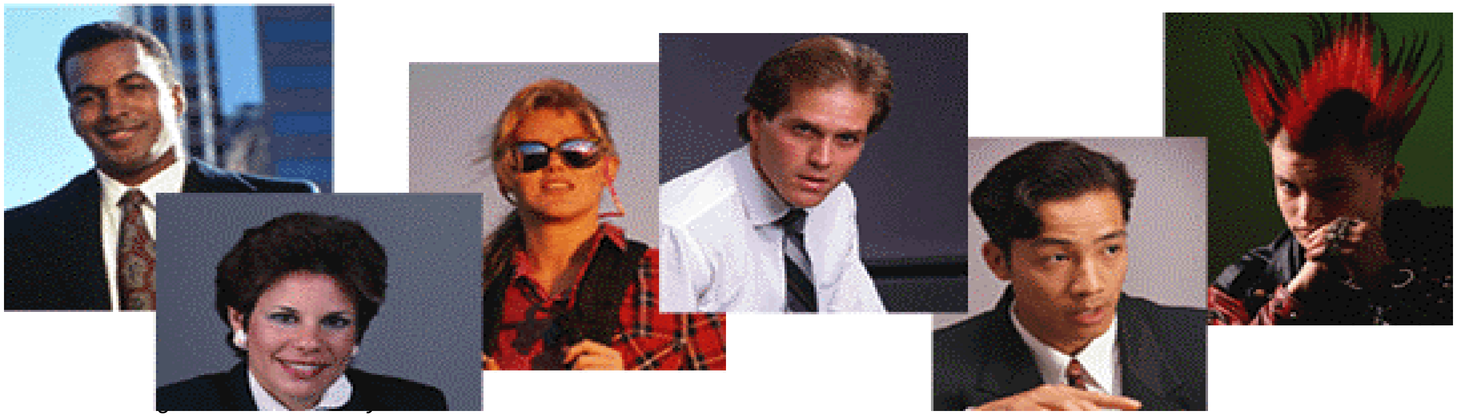
Increased Number of Incidents



More Sophisticated Intruders

Intruders are

- Building technical knowledge and skills
- Gaining leverage through automation
- Exploiting network interconnections and moving easily through the infrastructure
- Becoming more skilled at masking their behavior



Strain on System Administrators

There is continued movement to complex,client-server and heterogeneous configurations with distributed management

There is little evidence of security improvements in most products; new vulnerabilities are found routinely

Comprehensive security solutions are lacking; current tools address only parts of the problem

Strain on System Administrators

Engineering for ease of use has not been matched by engineering for ease of secure administration

- **ease of use and increased utility are driving a dramatic explosion in use**
- **system administration and security administration are more difficult than a decade ago**
- **this growing gap brings increased vulnerability**

Other Reasons for Concern

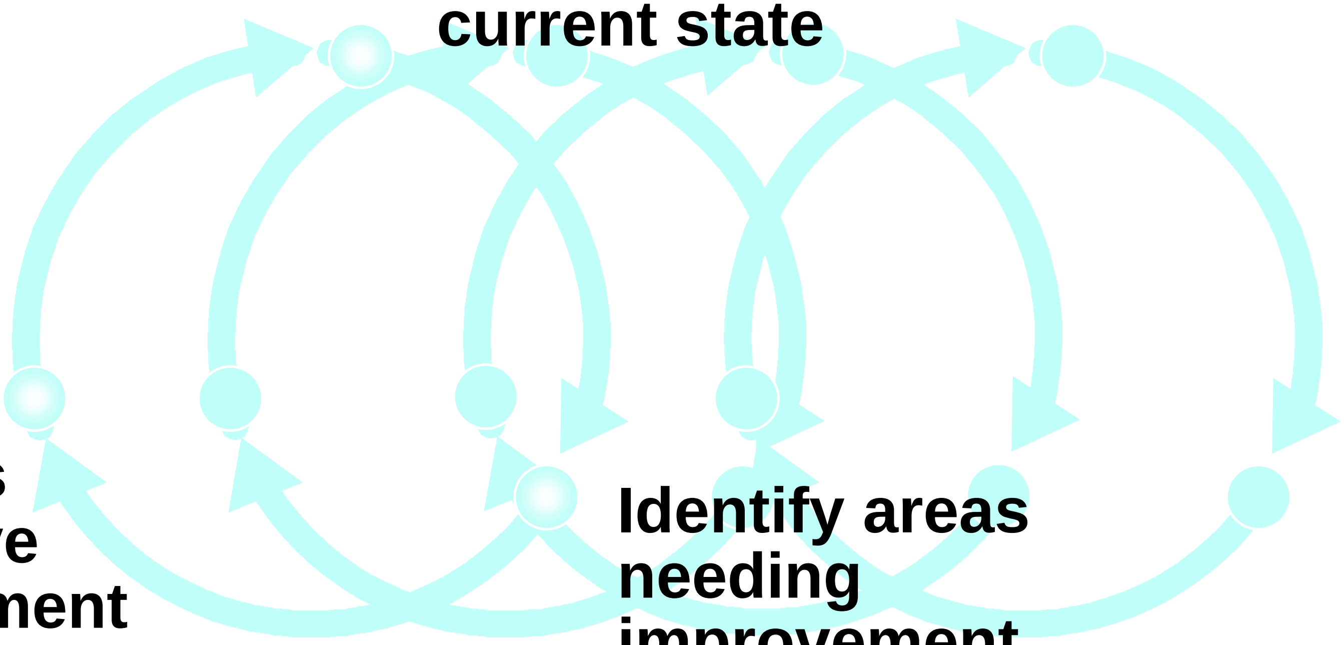
The demand for skilled system administrators far exceeds the supply

Many security audits and evaluations only skim the surface of the technology; major vulnerabilities are overlooked

Lack of understanding leads to reliance on partial solutions

What Can You Do to Make Your Networks More Secure?

Improvement Process



Assess current state

Apply practices to achieve improvement

Identify areas needing improvement

Start With Policy

Value your information and computing assets

- **What are they?**
- **How important is each one?**

Identification and authentication

Access

Privacy

Policy

Accountability

Violations reporting

Purchasing technology

Outsourcing

System and Security Architecture

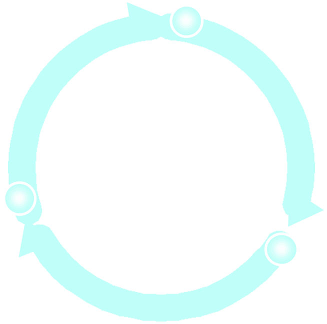
Perimeter controls

Internal partitioning to limit damage

Special protection for critical assets

Limit services to reduce risk

Instrumentation



Use available technology

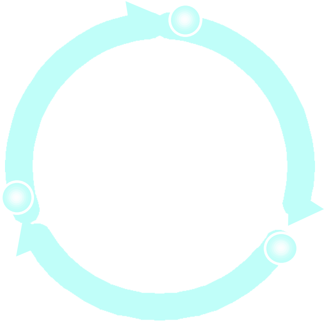
Authentication technology

Firewalls

Encryption

Virus detection

System & configuration management



Other important steps

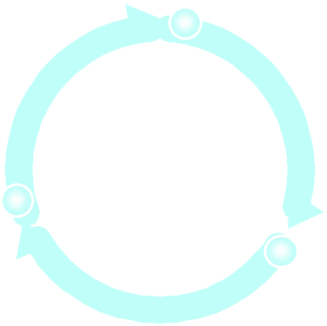
Training, training, training

- **users, managers, system administrators**

Maintain security awareness

Watch for changes

- **threats**
- **technology**
- **applications**
- **regulations and law**



Security is a process, not a state