CRITICAL INFRASTRUCTURE PROTECTION: THE LONG VIEW

Ken Watson

August 11, 2005

kwatson@cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

- Background – Critical Infrastructure Protection
- “Big” Challenges
- What’s Being Done?
- How Can I Get Involved?
- Cisco’s Commitment and Involvement
- Follow-up and Contact Information

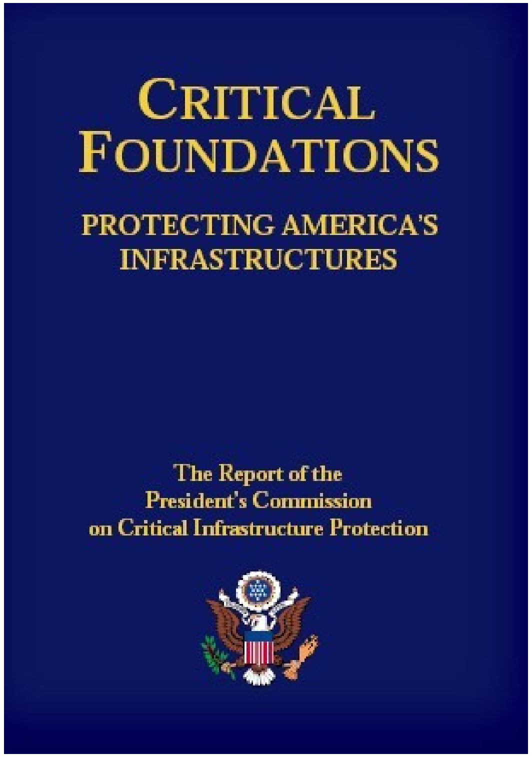
© 2005 Cisco Systems, Inc. All rights reserved.

CIP BACKGROUND

© 2005 Cisco Systems, Inc. All rights reserved.

President’s Commission on Critical Infrastructure Protection (CIP)

- 18-month study on critical infrastructure trends, vulnerabilities
- Led by Gen Robert Marsh (USAF, ret.)
- Published “Critical Foundations” October 1997
- Foundation of CIP initiative
- Driven by two trends
  - Government dependency on private sector
  - Migration to network-based operations



CRITICAL FOUNDATIONS

PROTECTING AMERICA'S INFRASTRUCTURES

The Report of the
President's Commission
on Critical Infrastructure Protection

© 2005 Cisco Systems, Inc. All rights reserved.

Business and Technology Trends

- Increasing government reliance on private sector infrastructure

  Governments purchasing communications, water, financial, health care, and transportation services from private sector

- Increasing reliance on networks

  Core business and government operations, not just e-mail and web sites

  Just-in-time supply chain management → increased productivity and efficiency

  Interdependencies mandate cross-sector and public-private planning and response

© 2005 Cisco Systems, Inc. All rights reserved.

Critical Infrastructures and Key Resources

- Banking & Finance
- Chemical
- Defense Industrial Base
- Emergency Services
- Energy
- Food & Agriculture
- Health Care
- Information Technology
- Postal & Shipping
- Telecommunications
- Transportation
- Water

© 2005 Cisco Systems, Inc. All rights reserved.

Critical Infrastructures and Key Resources

- Dams & Nuclear Power Plants
- Commercial Facilities
- Government Facilities
- National Monuments & Icons

© 2005 Cisco Systems, Inc. All rights reserved.

National Security Interest

- Critical infrastructures:
  - Are vital to safety, security, our way of life
  - Are largely owned and operated by private companies
- Defense Department:
  - Has no jurisdiction in private-sector networks
  - Has little visibility into threats to critical infrastructures
  - Must rely on private sector for defense against cyber attacks

Government needs industry in a true public-private partnership

© 2005 Cisco Systems, Inc. All rights reserved.

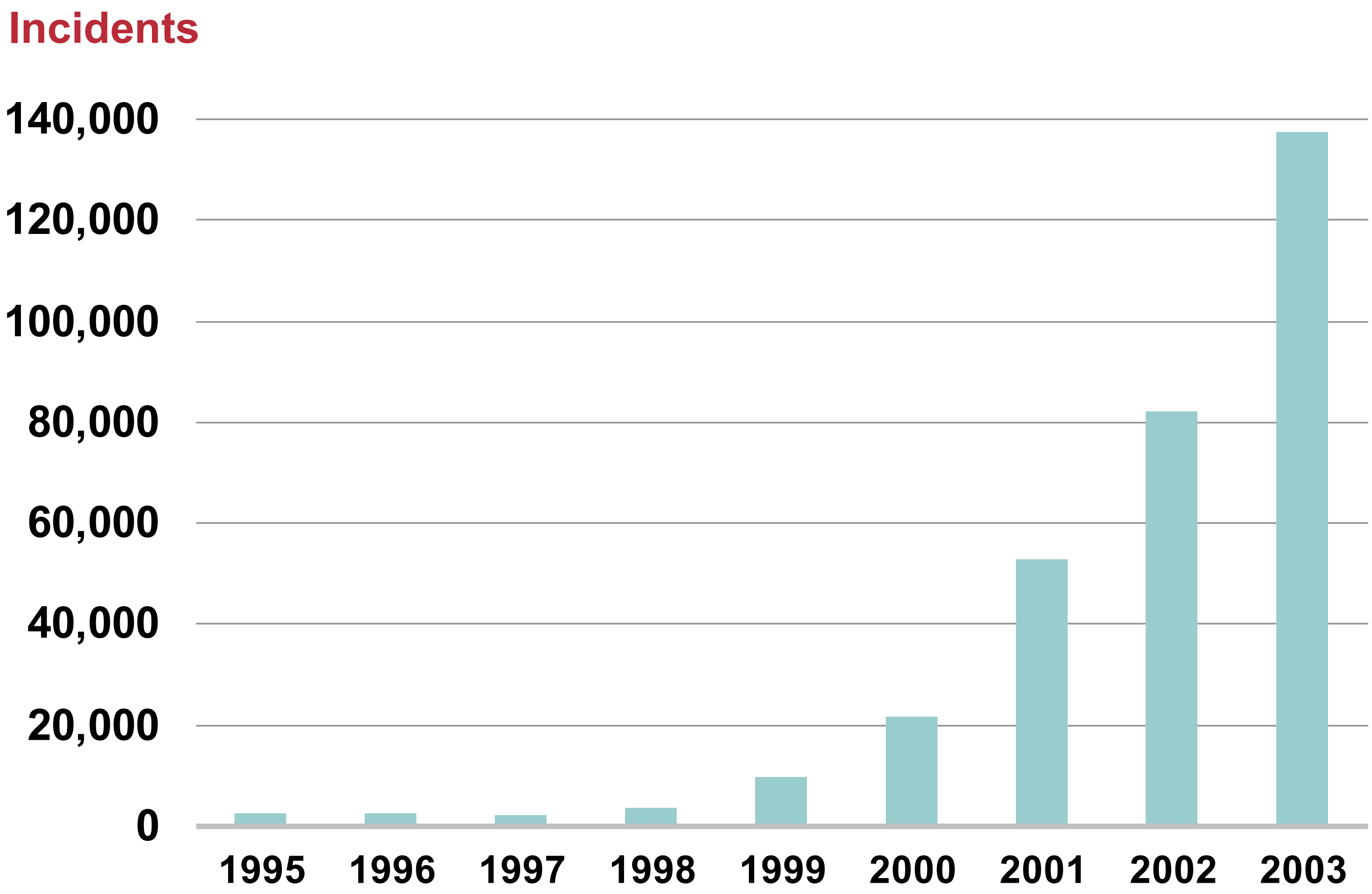
The Business Case

- Businesses depend on networks and rely on critical infrastructures
- Businesses familiar with interdependency
  - Supply chain
  - Partners
  - Customers
  - Infrastructure providers
- Unaddressed threats impact economic security and competitiveness
- National economic security integral to national security

Industry needs government in a true public-private partnership

© 2005 Cisco Systems, Inc. All rights reserved.

Security Incidents on the Rise

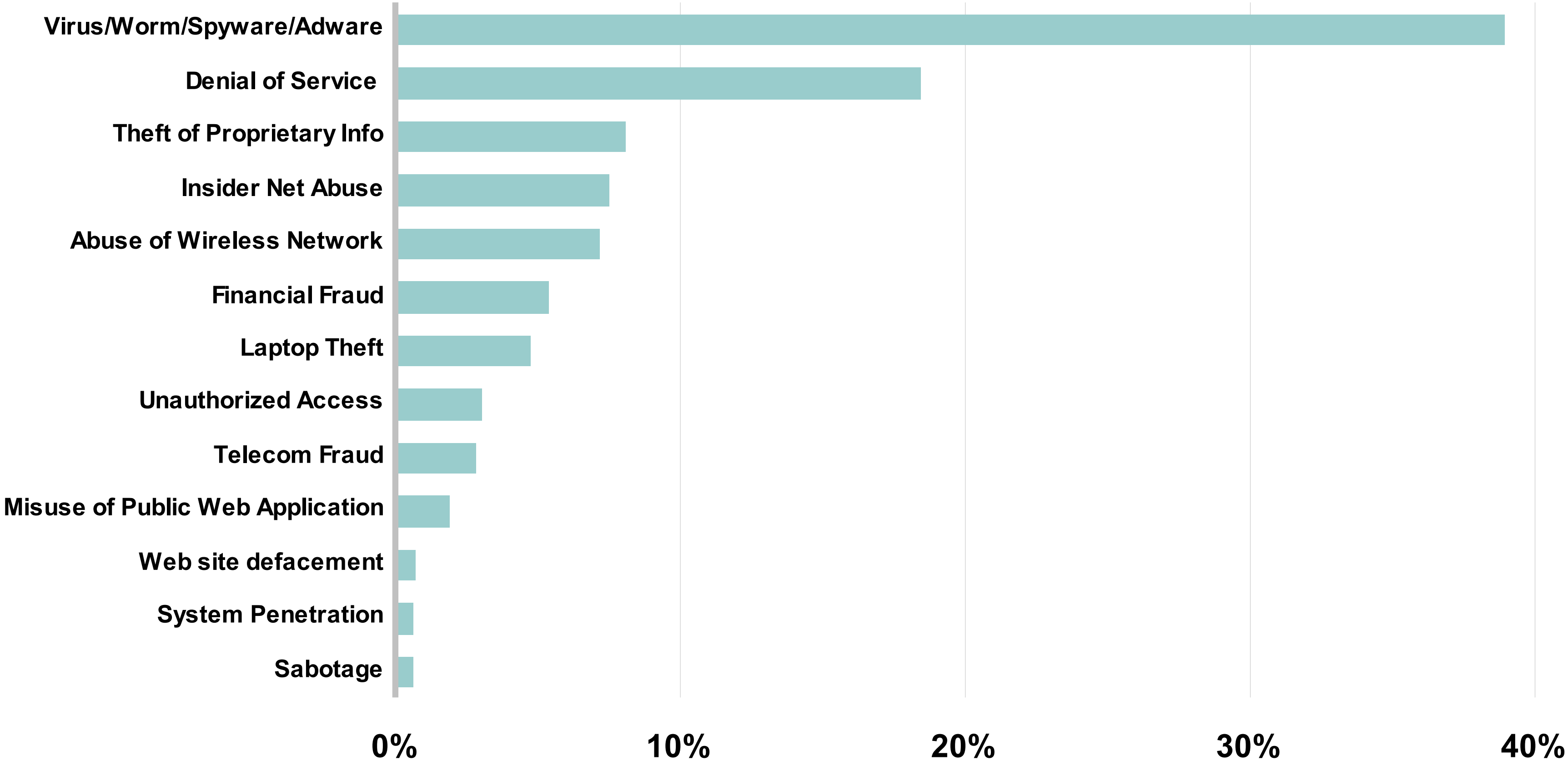


Source: CERT: Carnegie Mellon Software Engineering Institute, IDC

© 2005 Cisco Systems, Inc. All rights reserved.

Security Incidents Are Costly

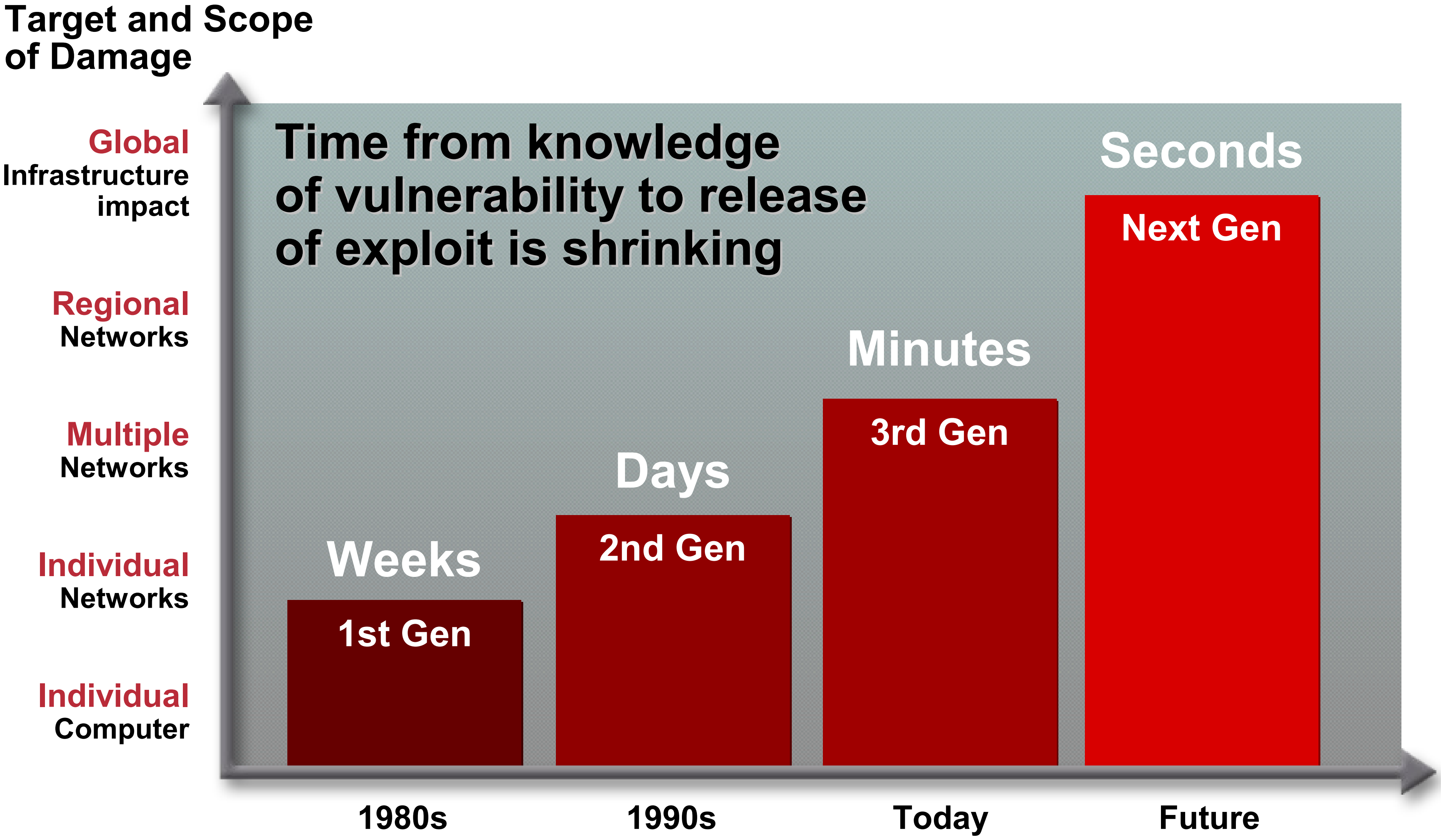
Loss Due to Computer Security Incidents



Source: CSI/FBI Computer Crime and Security Survey 2004

© 2005 Cisco Systems, Inc. All rights reserved.

Evolution of Security Challenges



© 2005 Cisco Systems, Inc. All rights reserved.

“BIG” CHALLENGES

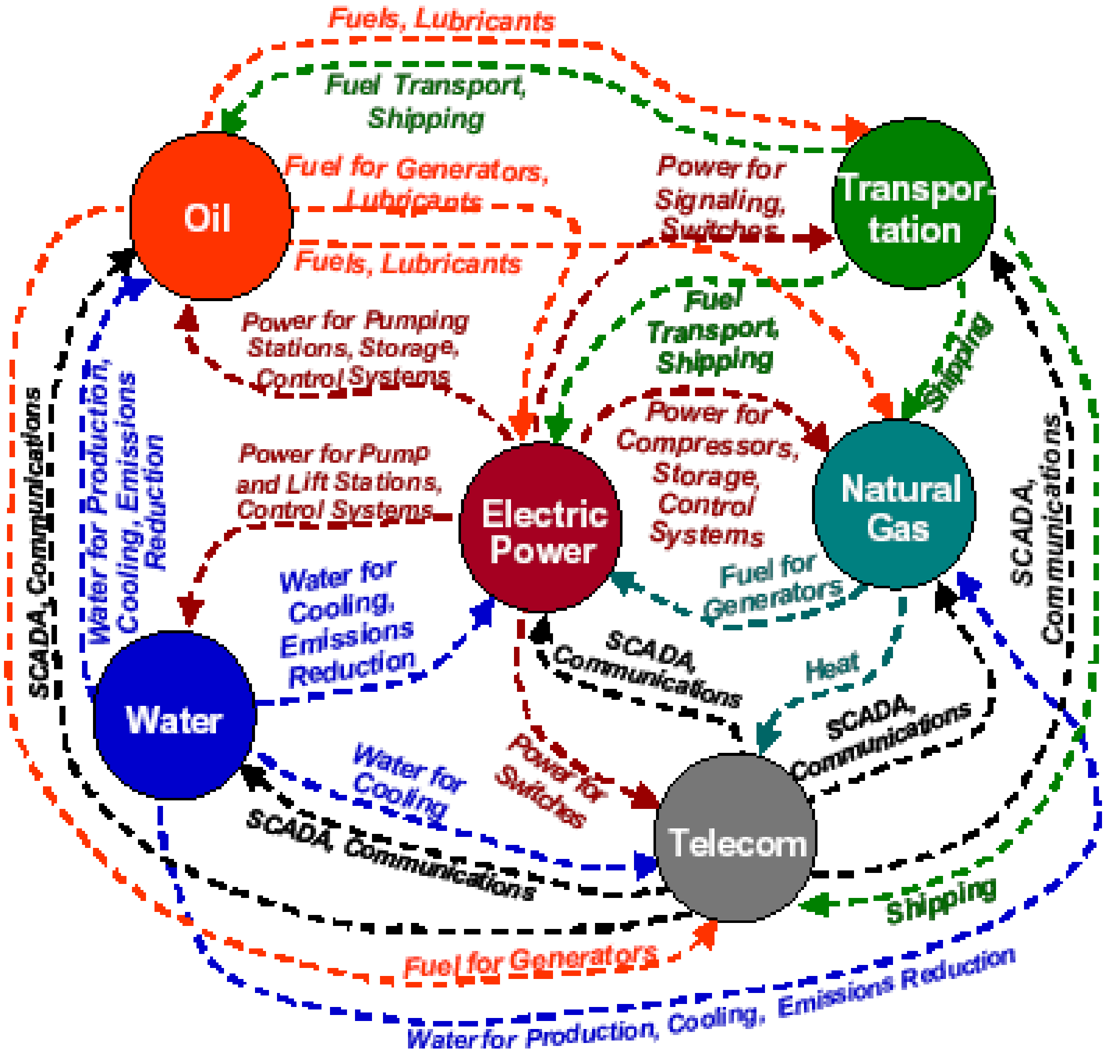
© 2005 Cisco Systems, Inc. All rights reserved.

“Big” Challenges

- Interdependency
- Identity management
- Internet and technology evolution
- Implications of convergence
- Software and system design
- Incident response coordination
- Law enforcement coordination

© 2005 Cisco Systems, Inc. All rights reserved.

Interdependency


Fuels, Lubricants
Fuel Transport, Shipping
Fuel for Generators, Lubricants
Fuels, Lubricants
Power for Signaling, Switches
Oil
Transportation
Power for Pumping Stations, Storage, Control Systems
Fuel Transport, Shipping
Shipping
Power for Compressors, Storage, Control Systems
Power for Pump and Lift Stations, Control Systems
Electric Power
Natural Gas
SCADA, Communications
Water for Production, Cooling, Emissions Reduction
SCADA, Communications
Fuel for Generators
Water for Cooling, Emissions Reduction
SCADA, Communications
Heat
SCADA, Communications
Water
Water for Cooling
Power for Switches
Telecom
SCADA, Communications
Shipping
Fuel for Generators
Water for Production, Cooling, Emissions Reduction

© 2005 Cisco Systems, Inc. All rights reserved.

Identity Management

- Access control
- Role-based trust
- Key management
- Identity without PKI?
- Identity integrity up and down the OCI model
- What about mobile, ad-hoc networks?
- Role of governments

© 2005 Cisco Systems, Inc. All rights reserved.

Internet and Technology Evolution

- Protocol security:
  - IPv6
  - BGP
  - DNS
  - SNMP
  - SCADA
  - Email protocols

- VoIP security
- Miniaturization
- Mobile ad-hoc networking
- Wireless everywhere
- Pervasive encryption
- Future Satellite-based communications

© 2005 Cisco Systems, Inc. All rights reserved.

Implications of Convergence

- Telecommunications & IT
- Physical & Cyber
- National & Economic Security

Common theme:

The Network

		Threats	
		Physical	Cyber
Targets	Physical	Bomb IED WMD	Control System, SCADA Hack
	Cyber	Backhoe	Virus Worm DDoS

© 2005 Cisco Systems, Inc. All rights reserved.

Software and System Design

- Assurance
- CS, EE curricula
- Programmer OJT
- Programming languages
- Standards documentation

© 2005 Cisco Systems, Inc. All rights reserved.

Incident Response Coordination

- Intelligence information (foreign)
- Law enforcement sensitive information (domestic)
- First-responder communications
- Site access management
- Regional exercises
- Incident triage

© 2005 Cisco Systems, Inc. All rights reserved.

Law Enforcement Coordination

- Information sharing
  - Intelligence Community
  - Law enforcement agencies
  - Critical infrastructure owners and operators
  - Public and press
- Jurisdictions
- Cross-border cooperation (extradition, investigations)
- Harmonization of criminal laws
- Harmonization of sentencing guidelines
- Chains of custody

© 2005 Cisco Systems, Inc. All rights reserved.

WHAT’S BEING DONE?

© 2005 Cisco Systems, Inc. All rights reserved.

Research

- **Government sponsoring research and articulating priorities**

  DHS, NSF, DARPA, HSARPA, OSTP

- **Industry conducting and sponsoring research**

- **Academia conducting research**

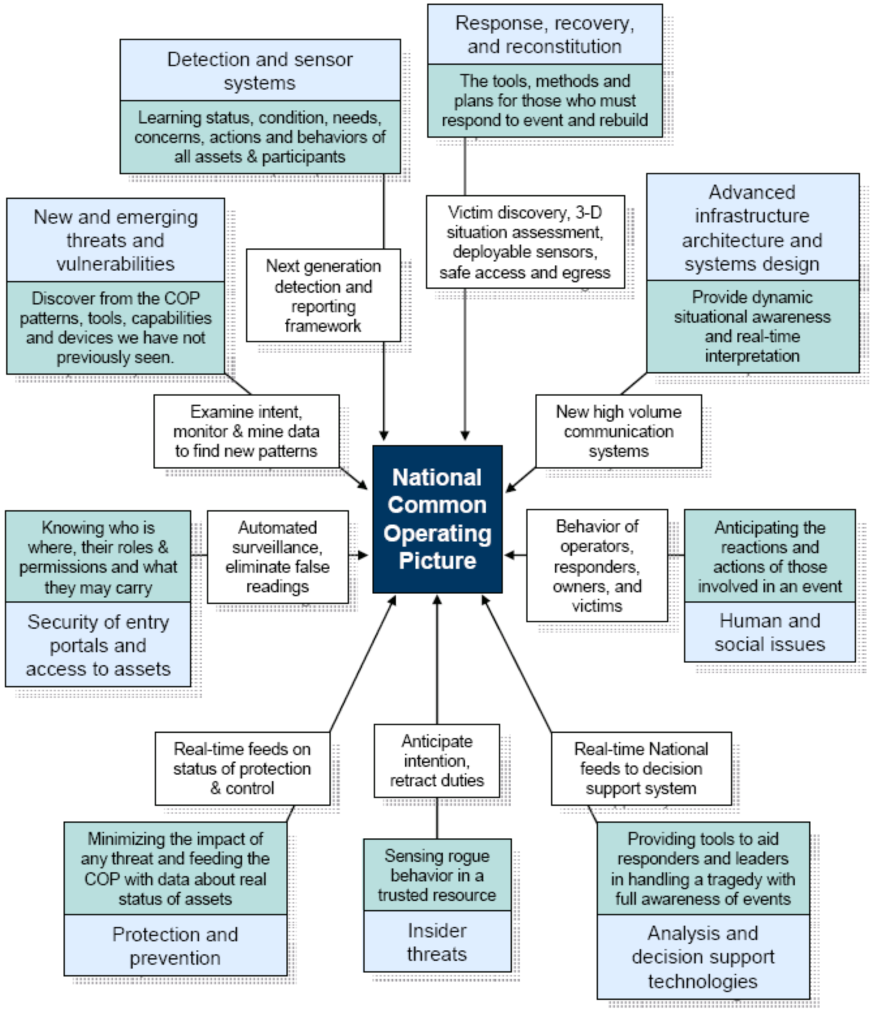
  Many, many universities

  Consortia and Centers

© 2005 Cisco Systems, Inc. All rights reserved.

DHS 2004 National CIP R&D Plan

- **April 8, 2005 Federal snapshot**
- **Evolving plan**
- **Acknowledges intersections among government, private sector, individuals**
- **Organized by theme, no sector**
- **Maps to other plans and strategies**
- **9 themes, 8 priorities**



National Common Operating Picture

Detection and sensor systems

Learning status, condition, needs, concerns, actions and behaviors of all assets & participants

Response, recovery, and reconstitution

The tools, methods and plans for those who must respond to event and rebuild

New and emerging threats and vulnerabilities

Discover from the COP patterns, tools, capabilities and devices we have not previously seen.

Next generation detection and reporting framework

Victim discovery, 3-D situation assessment, deployable sensors, safe access and egress

Advanced infrastructure architecture and systems design

Provide dynamic situational awareness and real-time interpretation

Examine intent, monitor & mine data to find new patterns

New high volume communication systems

Knowing who is where, their roles & permissions and what they may carry

Security of entry portals and access to assets

Automated surveillance, eliminate false readings

Behavior of operators, responders, owners, and victims

Anticipating the reactions and actions of those involved in an event

Human and social issues

Real-time feeds on status of protection & control

Anticipate intention, retract duties

Real-time National feeds to decision support system

Minimizing the impact of any threat and feeding the COP with data about real status of assets

Protection and prevention

Sensing rogue behavior in a trusted resource

Insider threats

Providing tools to aid responders and leaders in handling a tragedy with full awareness of events

Analysis and decision support technologies

© 2005 Cisco Systems, Inc. All rights reserved.

Institute for Information Infrastructure Protection (I3P)

- Dartmouth College
- Initial cyber security R&D Agenda, January 2003
- Multiple universities, labs, companies
- Sponsored by DHS and NIST
- Currently focusing on SCADA and financial aspects of CIP
- www.thei3p.org

© 2005 Cisco Systems, Inc. All rights reserved.

Rand CIP R&D Study

- "Cyber-Posture of the National Information Infrastructure"
- Sponsored by OSTP
- Complements President's Commission on Critical Infrastructure Protection report
- Identifies immediate, near-term, and mid-term actions
- Concentrates on information and communications, but includes discussion of interdependencies

© 2005 Cisco Systems, Inc. All rights reserved.

Industry efforts

- **NSTAC**
- **NIAC**
- **NRIC**
- **PCIS**
- **Cisco Systems**

© 2005 Cisco Systems, Inc. All rights reserved.

Workforce Development

- Institute for Defense Analyses Certification study
- DHS drive for “Common Body of Knowledge” approach
  - Software assurance
  - Individual certifications
- Curriculum development
- NSA/NIST/DHS Center of Excellence program
- Continuing education
- NIAC study

© 2005 Cisco Systems, Inc. All rights reserved.

IDA Certification Mapping Study

- Over 50 IA certification vendors
- Over 150 IA-related certifications
- 99 certifications applicable to DoD job categories
- Recommended standardizing job descriptions
  - 3 technical levels
  - 3 management levels
- Now working:
  - Performance-based testing
  - Test security
  - Developing metrics for ongoing assessments
- Collaborating with DHS, OPM for government-wide applicability

© 2005 Cisco Systems, Inc. All rights reserved.

Practices, Policy, and Standards Development

- NIAC
- NSTAC
- HSAC
- NRIC
- ANSI-HSSP
- ATIS
- IETF

© 2005 Cisco Systems, Inc. All rights reserved.

HOW CAN I GET INVOLVED?

© 2005 Cisco Systems, Inc. All rights reserved.

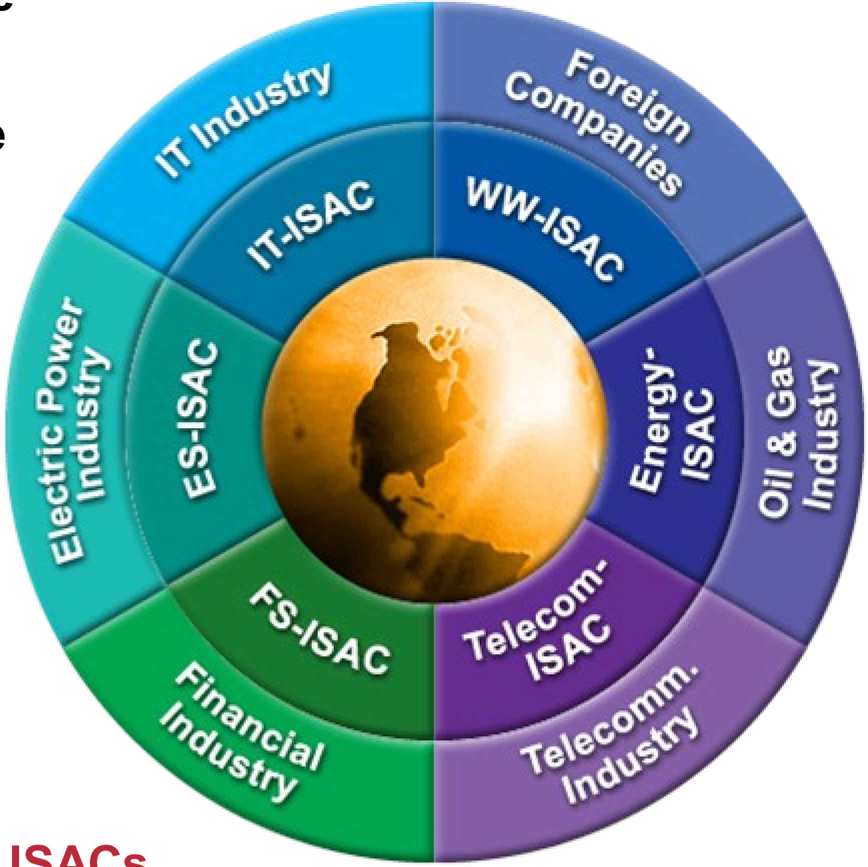
Partnership for Critical Infrastructure Security

- The forum for cross-sector CIP coordination
- Endorsed and sponsored by DHS
- Board of Directors composed of designated critical infrastructure “sector coordinators”

© 2005 Cisco Systems, Inc. All rights reserved.

Information Sharing and Analysis Centers (ISACs)

- Vital part of Critical Infrastructure Protection (CIP)
- Gather, analyze, and disseminate information on security threats, vulnerabilities, incidents, countermeasures, and best practices
- Early and trusted advance notification of member threats and attacks
- Organized by industry: cross-sector awareness, outreach, response and recovery
- ISAC Council: Leadership of ten ISACs



© 2005 Cisco Systems, Inc. All rights reserved.

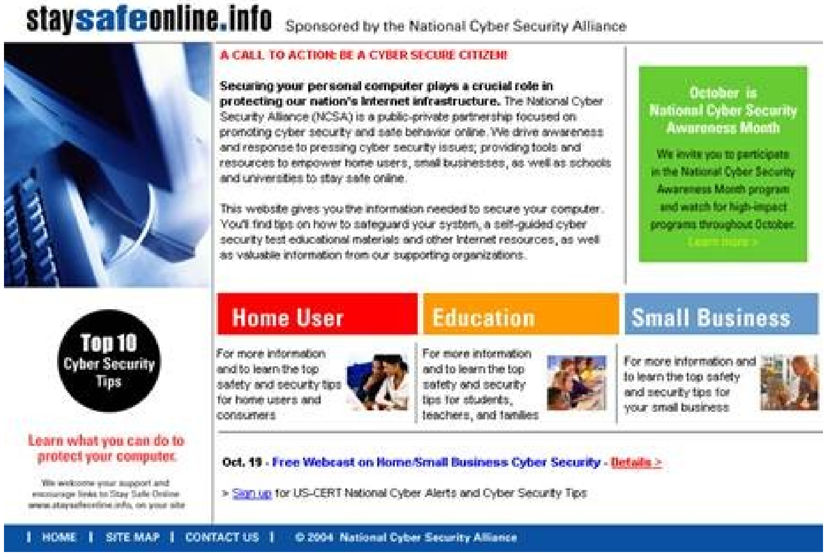
National Cyber Security Alliance

- Driving cyber security awareness and changing behavior
- Public service for:

  Home users

  Small businesses

  Schools (K-12), colleges, and universities
- Supported or endorsed by 50+ industry, government, & academic organizations
- October 2004: National Cyber Security Awareness Month
- DHS chose NCSA as its primary outreach vehicle for homes, small businesses, and schools



staysafeonline.info Sponsored by the National Cyber Security Alliance

A CALL TO ACTION: BE A CYBER SECURE CITIZEN!

Securing your personal computer plays a crucial role in protecting our nation's Internet infrastructure. The National Cyber Security Alliance (NCSA) is a public-private partnership focused on promoting cyber security and safe behavior online. We drive awareness and response to pressing cyber security issues; providing tools and resources to empower home users, small businesses, as well as schools and universities to stay safe online.

This website gives you the information needed to secure your computer. You'll find tips on how to safeguard your system, a self-guided cyber security test educational materials and other Internet resources, as well as valuable information from our supporting organizations.

October is National Cyber Security Awareness Month

We invite you to participate in the National Cyber Security Awareness Month program and watch for high-impact programs throughout October.

Learn more >

Top 10 Cyber Security Tips

Learn what you can do to protect your computer.

We welcome your support and encourage links to Stay Safe Online www.staysafeonline.info, on your site

Home User

For more information and to learn the top safety and security tips for home users and consumers

Education

For more information and to learn the top safety and security tips for students, teachers, and families

Small Business

For more information and to learn the top safety and security tips for your small business

Oct. 19 - Free Webcast on Home/Small Business Cyber Security - Details >

> Sign up for US-CERT National Cyber Alerts and Cyber Security Tips

| HOME | SITE MAP | CONTACT US | © 2004 National Cyber Security Alliance

www.staysafeonline.info

© 2005 Cisco Systems, Inc. All rights reserved.

National Infrastructure Advisory Council

- Composed of 30 CEOs or equivalents from all sectors
- Develops policy advice for the President
- Erle Nye, Chairman of TXU, is NIAC Chairman
- John Chambers, President and CEO of Cisco Systems, is NIAC Vice Chairman

© 2005 Cisco Systems, Inc. All rights reserved.

NIAC Reports Delivered to Date

- Internet Hardening
- Vulnerability Disclosure Framework
- Common Vulnerability Scoring System
- Cross-sector Interdependency and Risk Assessment
- Best Practices for Government Intervention
- Prioritization of Critical Infrastructure Sectors by Cyber Vulnerabilities
- Evaluation and Enhancement of Information Sharing and Analysis

© 2005 Cisco Systems, Inc. All rights reserved.

Infragard

- **Mission: improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures.**
- **Created in 1996**
- **68 of the top 100 firms in the Fortune 500 have an InfraGard representative**
- **Local chapter activities:**

  Training and education initiatives

  A local newsletter

  A Contingency Plan for using alternative systems in the event of a successful large scale attack on the information infrastructure
- **www.infragard.net**

© 2005 Cisco Systems, Inc. All rights reserved.

Industry Capabilities

- Innovate

  Improve and produce secure products and services

  (both security products and products that are secure)

- Develop technical and operational security best practices
- Adopt secure product design, implementation, testing, and deployment methodology
- Conduct and sponsor focused research
- Share information within and across sectors

  Threats, vulnerabilities, best practices, solutions

- Share information with government as appropriate

  Law enforcement investigations

  Vulnerability information (within constraints of PCII)

  Government must be able to protect this information

  Information must qualify for PCII (not otherwise required by government, etc.)

© 2005 Cisco Systems, Inc. All rights reserved.

Government Capabilities

- **Facilitate:** Get the right people talking to each other
- **Stimulate:** Provide incentives for network and equipment providers
- **Increase awareness:** Use the bully pulpit for good
- **Sponsor research:** Add public money to private to help solve the really hard problems
- **Use purchasing power:** Government can affect market as very large, powerful customer
- **Share information with industry:** Government plans or intelligence information can enhance public-private contingency planning and operations

© 2005 Cisco Systems, Inc. All rights reserved.

CISCO’S COMMITMENT AND INVOLVEMENT

© 2005 Cisco Systems, Inc. All rights reserved.

Cisco's Leadership in Critical Infrastructure Protection (CIP)

- National Infrastructure Advisory Council (NIAC) (Vice Chairman)
- Partnership for Critical Infrastructure Security
- IT & Telecom ISACs
- National Cyber Security Alliance (Chairman)
- Colloquium for Information Systems Security Education (CISSE)
- Committee on National Security Systems (CNSS)
- American National Standards Institute Homeland Security Standards Panel (ANSI-HSSP)
- National Emergency Numbers Association (NENA)
- National Center for Manufacturing Sciences
- Forum of Incident Response and Security Teams (FIRST) (Steering Committee)
- National Institute for Urban Search and Rescue (NIUSR) (Exec Board)
- Multiple CIP research relationships
- Alliance for Telecommunications Industry Solutions (ATIS) TOPS
- Network Reliability and Interoperability Council
- Network Service Provider Security (NSP-SEC) initiative

© 2005 Cisco Systems, Inc. All rights reserved.

Cisco's Critical Infrastructure Assurance Group (CIAG)

Mission

Develop and implement homeland security and critical infrastructure assurance programs by leveraging Cisco's expertise in computing and network security

Program Areas

- Research
- Workforce Development
- Practices, Policies, and Standards Development

www.cisco.com/go/ciag

© 2005 Cisco Systems, Inc. All rights reserved.

Cisco CIAG Research Program: Selected Projects

Research Area	Project Titles
Secure Coding	eRFC Networking software engineering security best practices
Malware Protection	Internet Motion Sensor Worm Simulation
Industrial Network Security	AGA Link Encryption Protocol SCADA Firewall and Honeynet Sensor Hardening Airplane Networks Security
Physical/Cyber Security	BACnet Best Practices
Internet Routing Protocols Security	IPv6 Security Routing Validation Graphs for interdomain routing BGP Security
People, Process and Policy aspects of Security	CVSS Active Defense
Internet Infrastructure Security	DNS Security Internet Hardening Route Registries Enhancement ASN Whois Enhancement

© 2005 Cisco Systems, Inc. All rights reserved.

Workforce Development
Industry & Government Support

- Securing Cisco Routers (SECR) v1.0

  Free online training covering 10 best practices recommended for securely configuring Cisco routers

  www.cisco.com/security/secr

- Industry Bootcamps – Rural Electric Cooperatives

  4 day hands-on security course offered free to IA professionals where Critical Infrastructure is impacted

  Content includes router security, VPN, firewalls, & IDS

- Cisco SECUR certification mapped to government CNSS 4011 Standard – makes Cisco certifications interchangeable between the public & private sector

© 2005 Cisco Systems, Inc. All rights reserved.

Food for Thought

- National, economic security forever intertwined
- Infrastructures are interdependent
- Companies, governments, and academia must work together
- Public-private partnership is the new norm
- Each partner’s core competencies are strengths

© 2005 Cisco Systems, Inc. All rights reserved.

Follow-up and Contacts

- Partnership for Critical Infrastructure Security

  Rod Nydam Executive Director

  703-993-4861

  rnydam@gmu.edu

- Information Sharing and Analysis Centers

  www.isaccouncil.org

  pallor@iss.net

- National Cyber Security Alliance

  Ron Teixeira, Executive Director

  202-331-5350

  NCSARon@aol.com

- Infragard Omaha

  402-492-3772

  infragard-omaha@infragard.c

Ken Watson
512-378-1112
kwatson@cisco.com
www.cisco.com/go/ciag

© 2005 Cisco Systems, Inc. All rights reserved.

Q and A

http://www.cisco.com/go/ciag

© 2005 Cisco Systems, Inc. All rights reserved.

CISCO SYSTEMS ®

© 2004 Cisco Systems, Inc. All rights reserved.

© 2005 Cisco Systems, Inc. All rights reserved.

48