The Challenging Landscape of Critical Information Infrastructure:

Are We Ready?

Leonard Bailey
Senior Counsel
Computer Crime &
Intellectual Property Section
US Department of Justice
March 9, 2007

Agenda|

- Define the challenge.
- Outline the response.
- Propose ways forward.

Define the challenge.

The Complicated Landscape of Critical Information Infrastructure Protection:

Are We Ready?

The Complicated Landscape of Critical Information Infrastructure Protection:

Are We Ready?

Private v. Public

International

Physical v. Cyber

Military v. Non-Military Systems

Wartime v. Peacetime

Cyber Disaster Planning|

- Federal Incident Response Community
  - DHS, National Cyber Security Division
  - Law Enforcement/Intel
  - Department of Defense
- Information Sharing and Analysis Centers
- Sector Coordinating Councils
- Government Coordinating Council
- International Entities

The Complicated Landscape of Critical Information Infrastructure Protection:

Are We Ready?

13 Critical Infrastructure Sectors

The Complicated Landscape of Critical Information Infrastructure Protection:

Are We Ready?

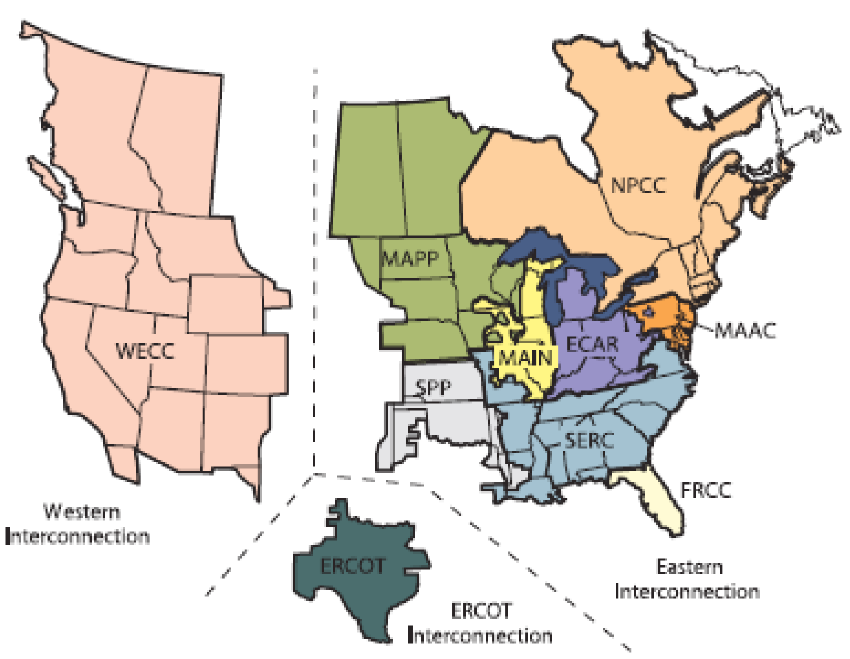
Communications and IT Sectors

What is "Critical"?

- Executive Order 13010
  - "Infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security."
- USA PATRIOT Act (P.L. 107-56)
  - "[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

What is “Critical”?

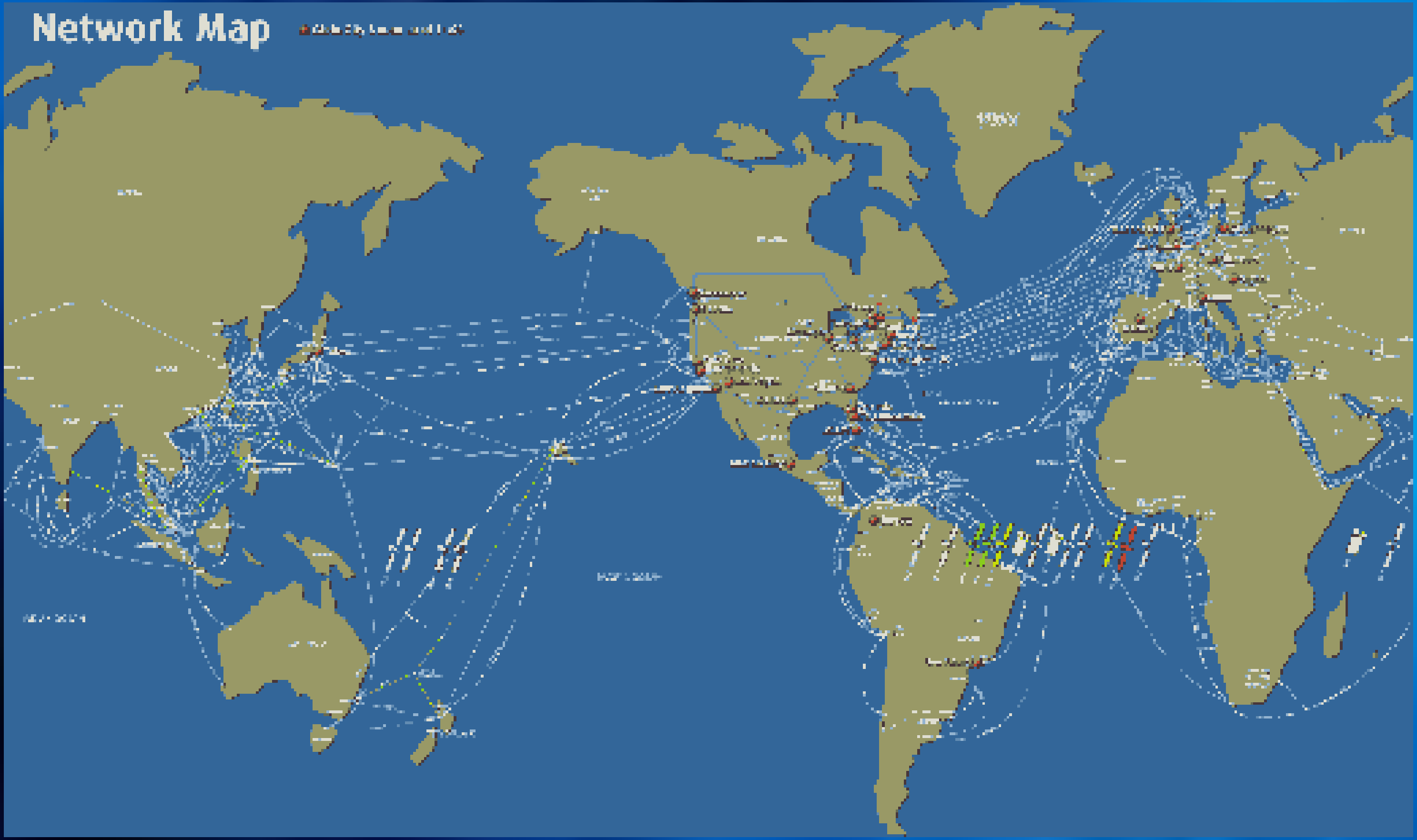
- Interdependencies between Sectors
  - Known, unknown and unknowable.
- Interconnected systems
  - “The North American power grid is one large, interconnected machine.”



What is “Critical”?

- Convergence
  - Progress toward integrated IP Network.
  - Increased opportunity for cascading failure.
  - New “critical” functions.

International



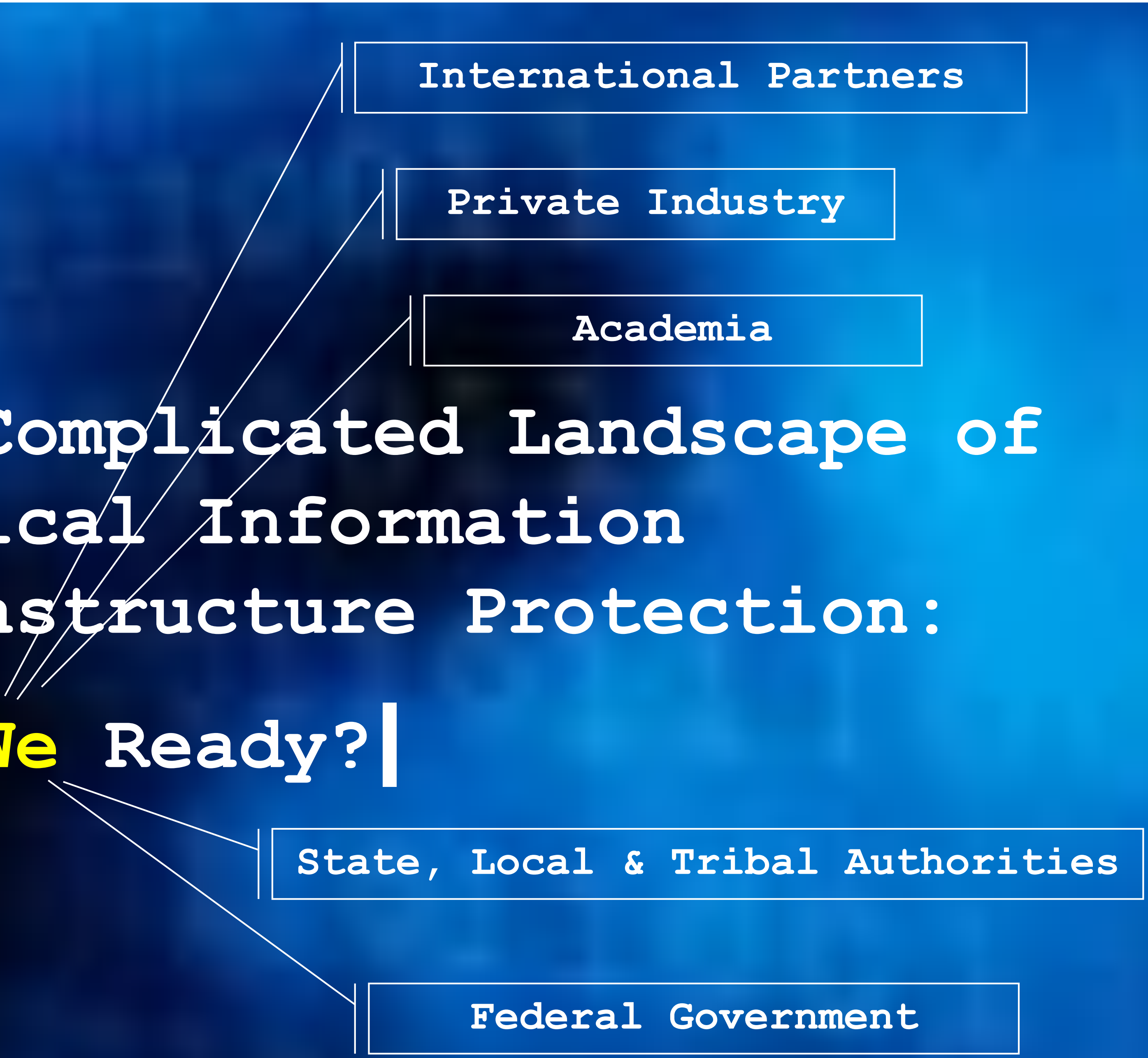
Outline the response.

The Complicated Landscape of Critical Information Infrastructure Protection:

Are We Ready?

The Complicated Landscape of Critical Information Infrastructure Protection:

Are We Ready?



International Partners

Private Industry

Academia

State, Local & Tribal Authorities

Federal Government

Natural Disaster

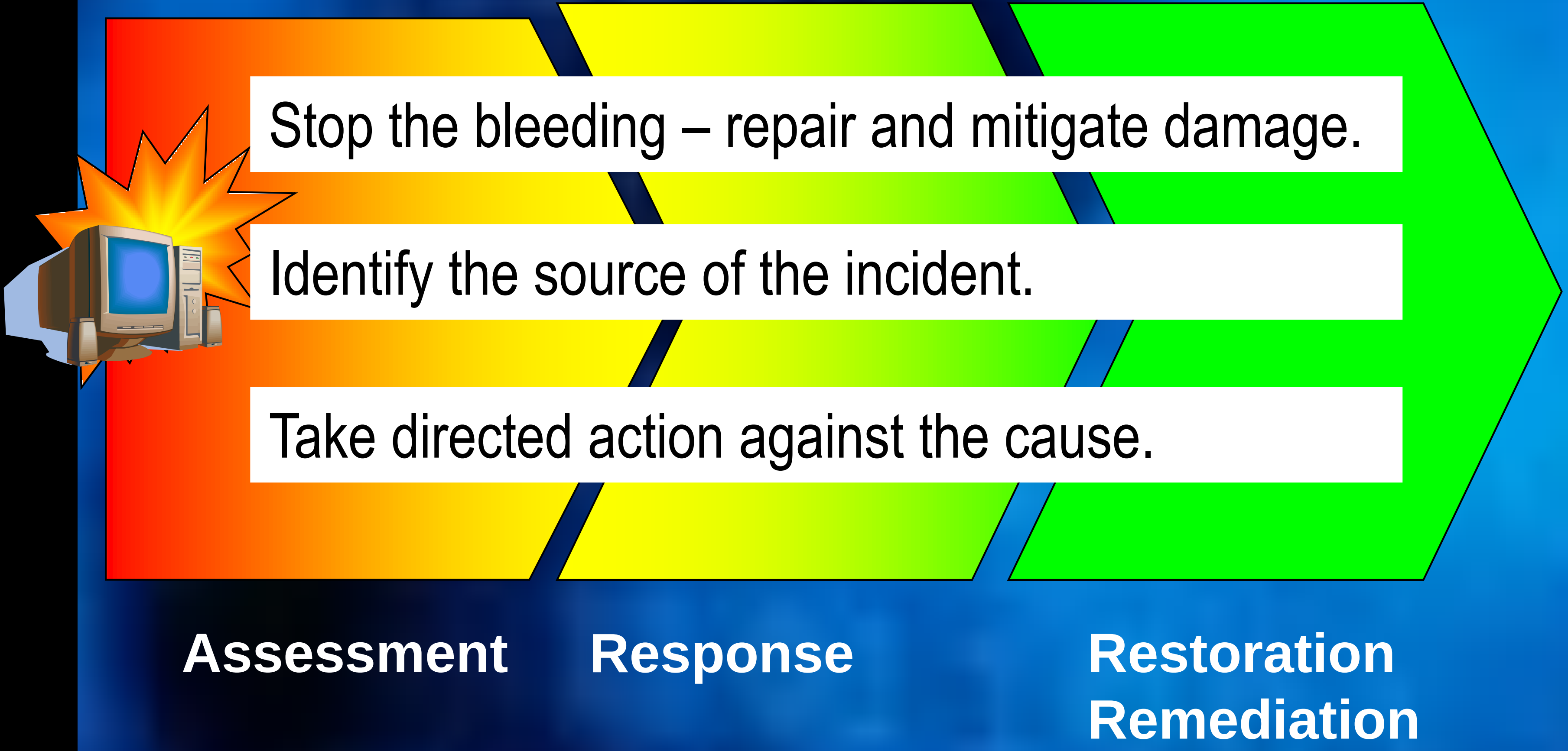
The Complicated Landscape of Critical Information Infrastructure Protection:

Are We Ready?

Attack

Accident

Incident Response

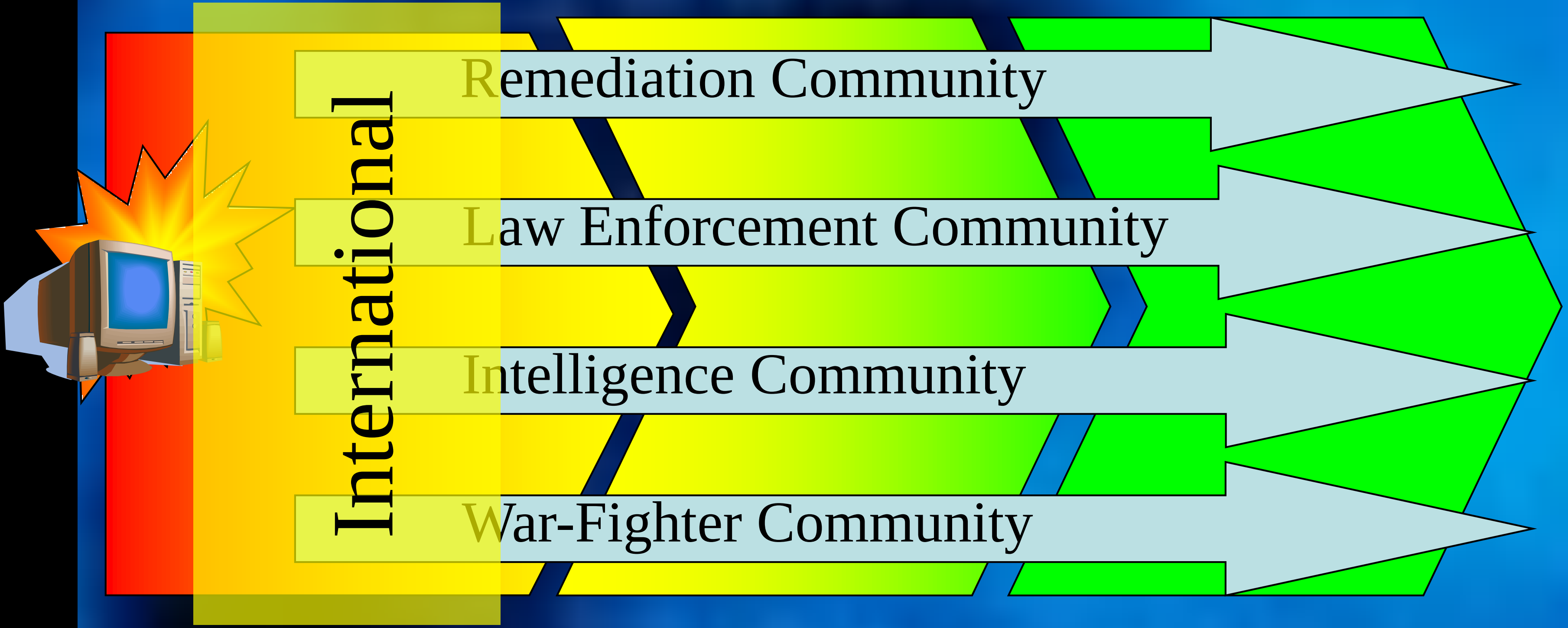


Stop the bleeding – repair and mitigate damage.

Identify the source of the incident.

Take directed action against the cause.

Incident Response



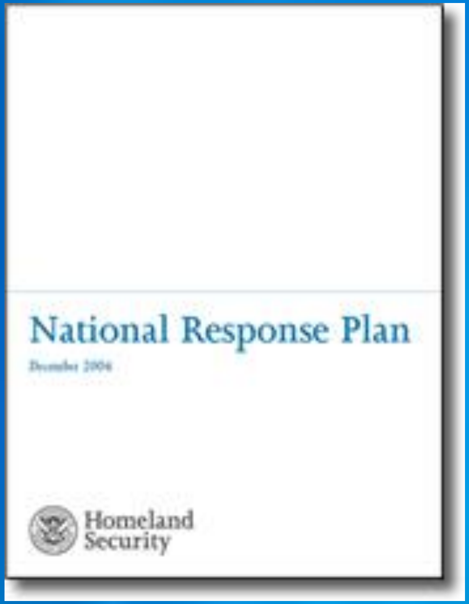
Assessment

Response

Restoration
Remediation

Tripwires

- National Response Plan
  - The National Response Plan establishes a comprehensive approach to enhance the ability of the United States to manage domestic incidents.
  - Homeland Security Policy Directive 5
  - Signed December 2004.



National Response Plan

December 2004

Homeland Security

Tripwires

- "Incident of national significance"
  - An actual or potential high-impact event that requires a coordinated and effective response by and appropriate combination of Federal, State, local, tribal, nongovernmental, and/or private-sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities.
  - Cyber Annex specifically addresses management of cyber incidents.

National Cyber Response Coordination Group

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

U.S. DEPARTMENT OF HOMELAND SECURITY

DEPARTMENT OF JUSTICE

Origin of the NCRCG |

- Department of Homeland Security
  - Effectuate responsibilities under HSPDs 5 and 7 and the National Response Plan (NRP).
- Department of Justice
  - Replace the IRC with an operational group that could help coordinate investigative response activities during a cyber incident.
- National Security Council
  - Provide a central interagency group for addressing cyber issues implicating national and homeland security.

Structure of the NCRCG|

- Steering Committee
  - Co-chaired by DHS/NCSD, DOJ/CCIPS, and DOD/OSD-NII.
  - Includes:
    - CIA
    - DHS
    - Director of National Intelligence (DNI)
    - DOD
    - DOE
    - DOJ
    - HSC
    - NCIX
    - NSA
    - NSC
    - OMB

Propose ways forward.

What you can do|

- Encourage your leadership to undertake the challenge.

What you can do|

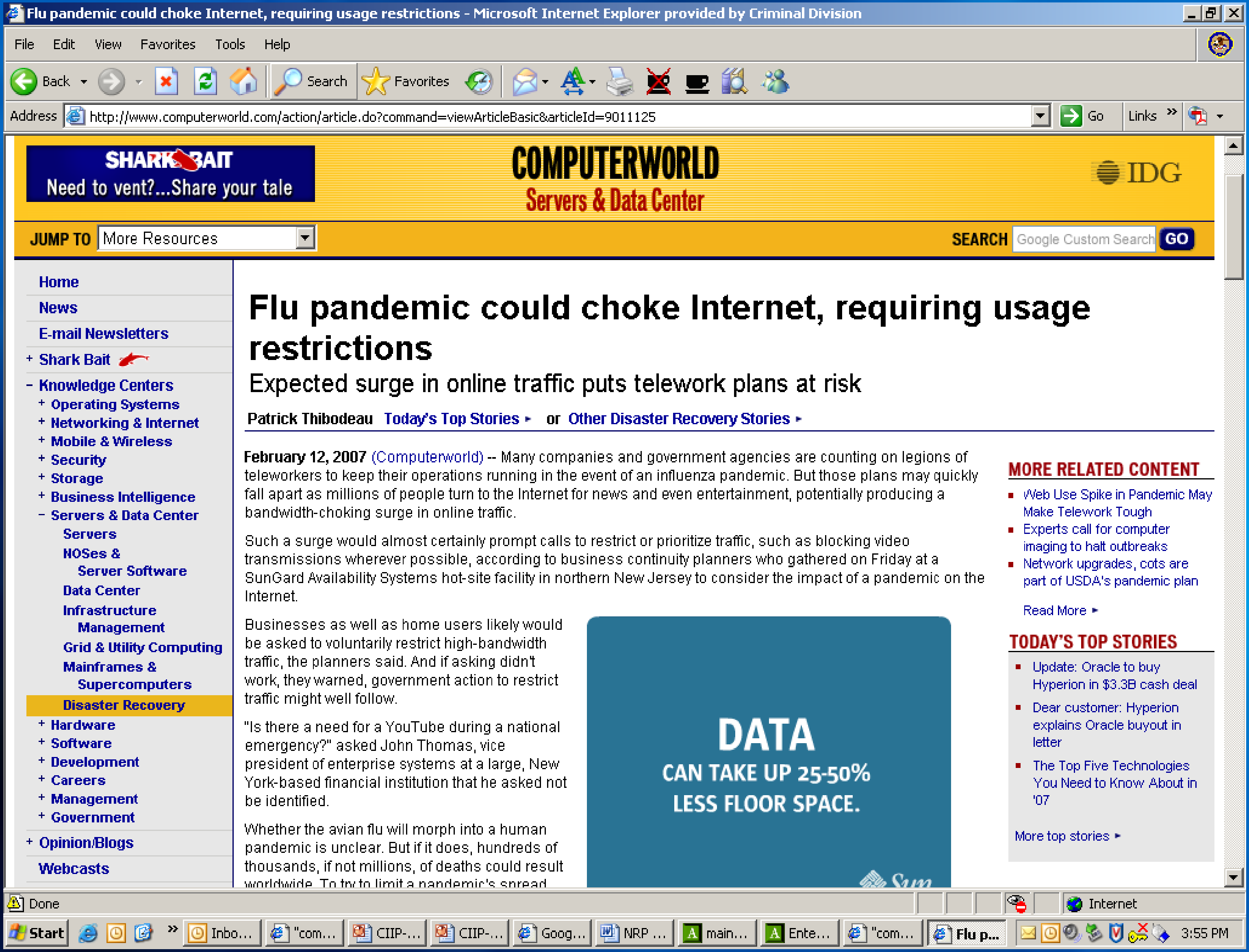
- Challenge your leadership.
  - Help them focus on what matters in a manner that is helpful to them.

What you can do|

- Align words and deeds
  - Are your entity's actions consistent with the perception of the threat?
  - If not, why not?

What you can do|

- Prepare and practice.
  - Do you have an incident response plan?
  - Is it up-to-date?
  - Has it been socialized in your organization?
  - Are you confident that it will be followed?


Flu pandemic could choke Internet, requiring usage restrictions - Microsoft Internet Explorer provided by Criminal Division
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011125
Go
Links
Done
Internet
Start
Inbo...
"com...
CIIP-...
CIIP-...
Goog...
NRP ...
main...
Ente...
"com...
Flu p...
3:55 PM

COMPUTERWORLD
Servers & Data Center

IDG

JUMP TO More Resources

SEARCH Google Custom Search GO

- Home
- News
- E-mail Newsletters
- + Shark Bait
- − Knowledge Centers
  - + Operating Systems
  - + Networking & Internet
  - + Mobile & Wireless
  - + Security
  - + Storage
  - + Business Intelligence
  - − Servers & Data Center
    - Servers
    - NOSes & Server Software
    - Data Center
    - Infrastructure Management
    - Grid & Utility Computing
    - Mainframes & Supercomputers
    - Disaster Recovery
  - + Hardware
  - + Software
  - + Development
  - + Careers
  - + Management
  - + Government
- + Opinion/Blogs
- Webcasts

Flu pandemic could choke Internet, requiring usage restrictions

Expected surge in online traffic puts telework plans at risk

Patrick Thibodeau Today's Top Stories ▸ or Other Disaster Recovery Stories ▸

February 12, 2007 (Computerworld) -- Many companies and government agencies are counting on legions of teleworkers to keep their operations running in the event of an influenza pandemic. But those plans may quickly fall apart as millions of people turn to the Internet for news and even entertainment, potentially producing a bandwidth-choking surge in online traffic.

Such a surge would almost certainly prompt calls to restrict or prioritize traffic, such as blocking video transmissions wherever possible, according to business continuity planners who gathered on Friday at a SunGard Availability Systems hot-site facility in northern New Jersey to consider the impact of a pandemic on the Internet.

Businesses as well as home users likely would be asked to voluntarily restrict high-bandwidth traffic, the planners said. And if asking didn't work, they warned, government action to restrict traffic might well follow.

"Is there a need for a YouTube during a national emergency?" asked John Thomas, vice president of enterprise systems at a large, New York-based financial institution that he asked not be identified.

Whether the avian flu will morph into a human pandemic is unclear. But if it does, hundreds of thousands, if not millions, of deaths could result worldwide. To try to limit a pandemic's spread

MORE RELATED CONTENT

- Web Use Spike in Pandemic May Make Telework Tough
- Experts call for computer imaging to halt outbreaks
- Network upgrades, cots are part of USDA's pandemic plan

Read More ▸

TODAY'S TOP STORIES

- Update: Oracle to buy Hyperion in $3.3B cash deal
- Dear customer: Hyperion explains Oracle buyout in letter
- The Top Five Technologies You Need to Know About in '07

More top stories ▸

Getting more info

- Contact Us
  - Main: (202) 514-1026
  - E-Mail: leonard.bailey@usdoj.gov
- Web:

WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice