DIR
Department of Information Resources

State Enterprise Security Update
Department of Information Resources

Before the Senate Committee on
Transportation and Homeland Security

June 8, 2010

Defining Information Security

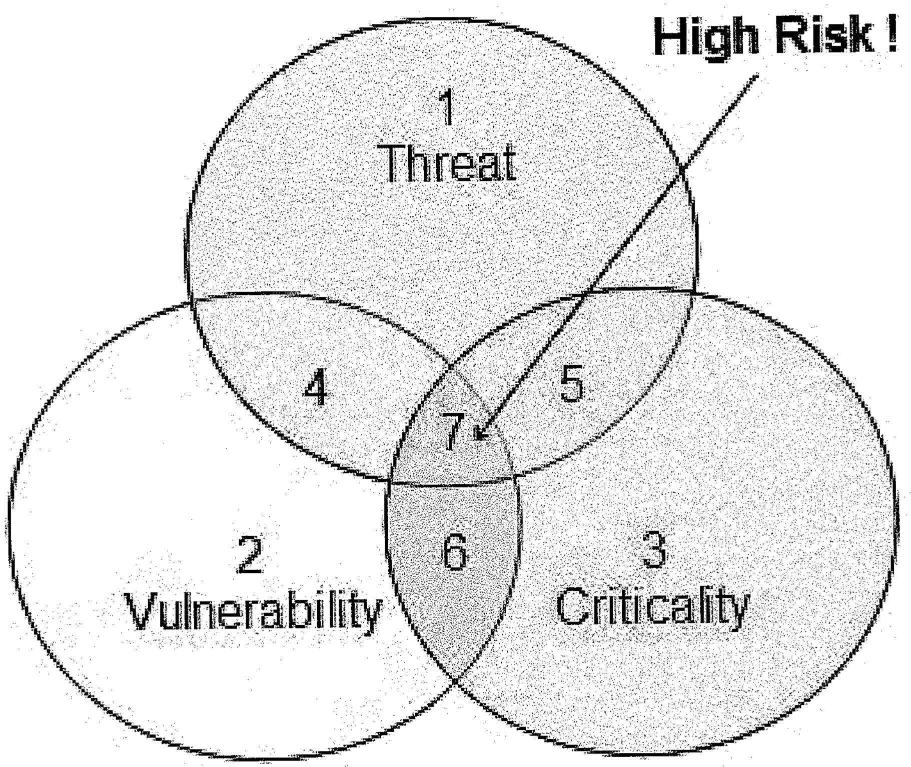
- **Information Security (InfoSec) is defined as:**

  Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide [integrity, confidentiality, and availability]*

- **Note the focus on information and systems, not just computers**

* From U.S. Code Title 44, Chapter 35, Subchapter III, § 3542, Definitions, b.1

Cornerstone of Security: Managing Risk



The Context of Risky Situations

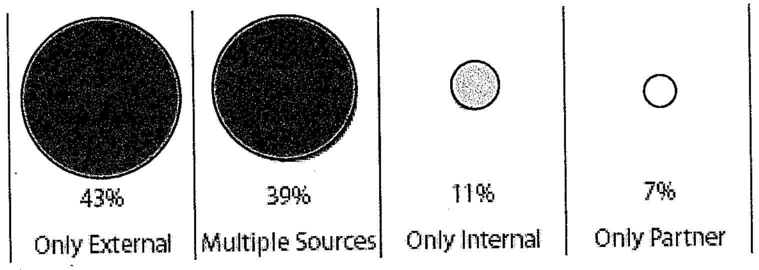
Scope of Problem

- FY 2009 – State of Texas agencies and universities reported a daily average of 575 security incidents
- Jan 2005 to Aug 2009 – Texas-based orgs reported by Privacy Clearinghouse:
  - 105 incidents involving privacy data (43 state gov incidents)
  - 3+ million individual records exposed (+12% of the state's population)
  - Estimated cost of $202 per record exposed
  - Totaling $606 million dollars to recover from the attacks

Source: *Texas Homeland Security Strategic Plan, 2005-2010*

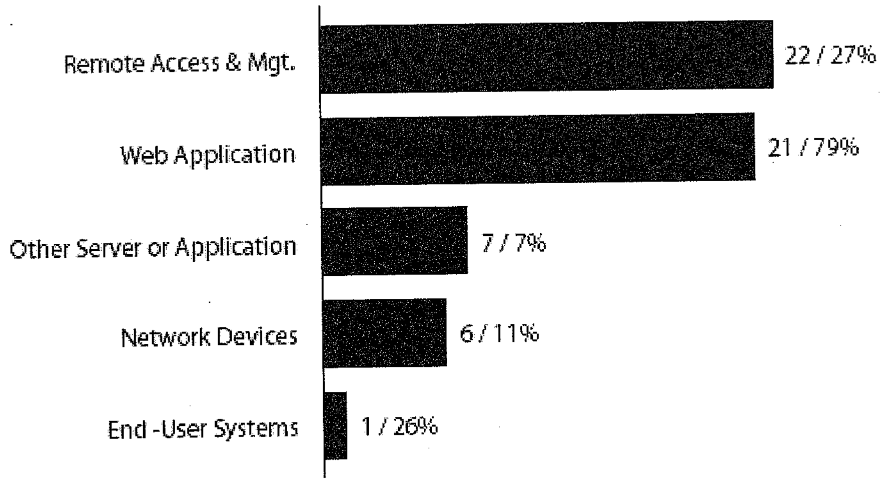
Relative Risk of External vs Internal Threats

Single vs. multiple breach sources by percent of breaches



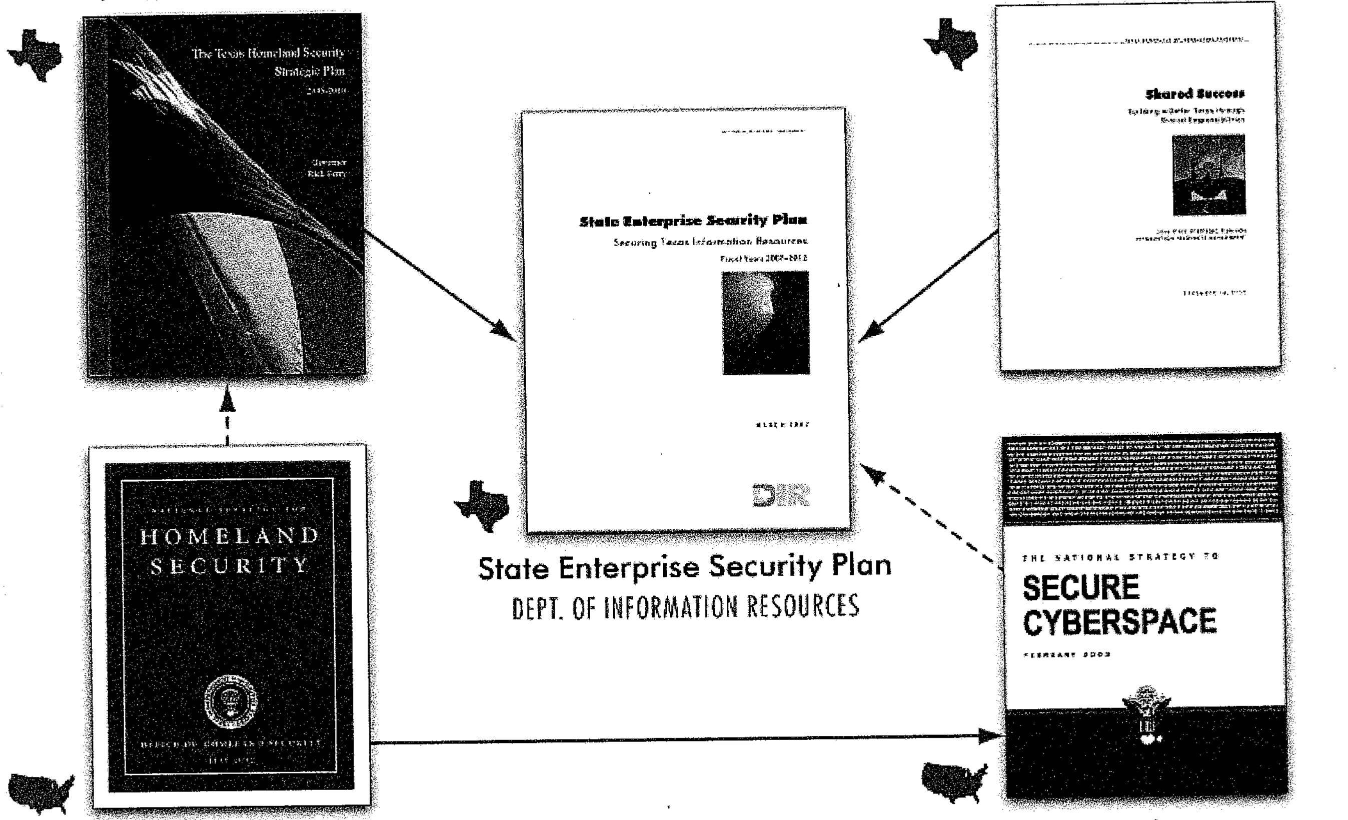
"Results from 600 incidents over 5 years make a strong case against the long-abiding and deeply held belief that insiders are behind most breaches."

Attack pathways by number of breaches (black) and percent of records (red)



Source: 2009 Data Breach Investigations Report, Verizon Business RISK Team

Security Plan



The Texas Homeland Security Strategic Plan
HOMELAND SECURITY
State Enterprise Security Plan
Securing Texas Information Resources
Shared Success
THE NATIONAL STRATEGY TO SECURE CYBERSPACE
FEBRUARY 2003
DIR

Texas Homeland Security
Strategic Plan (TxHSSP)
OFFICE OF THE GOVERNOR

2005 State Strategic Plan for
Information Resources Mgmt (SSP)
DEPT. OF INFORMATION RESOURCES

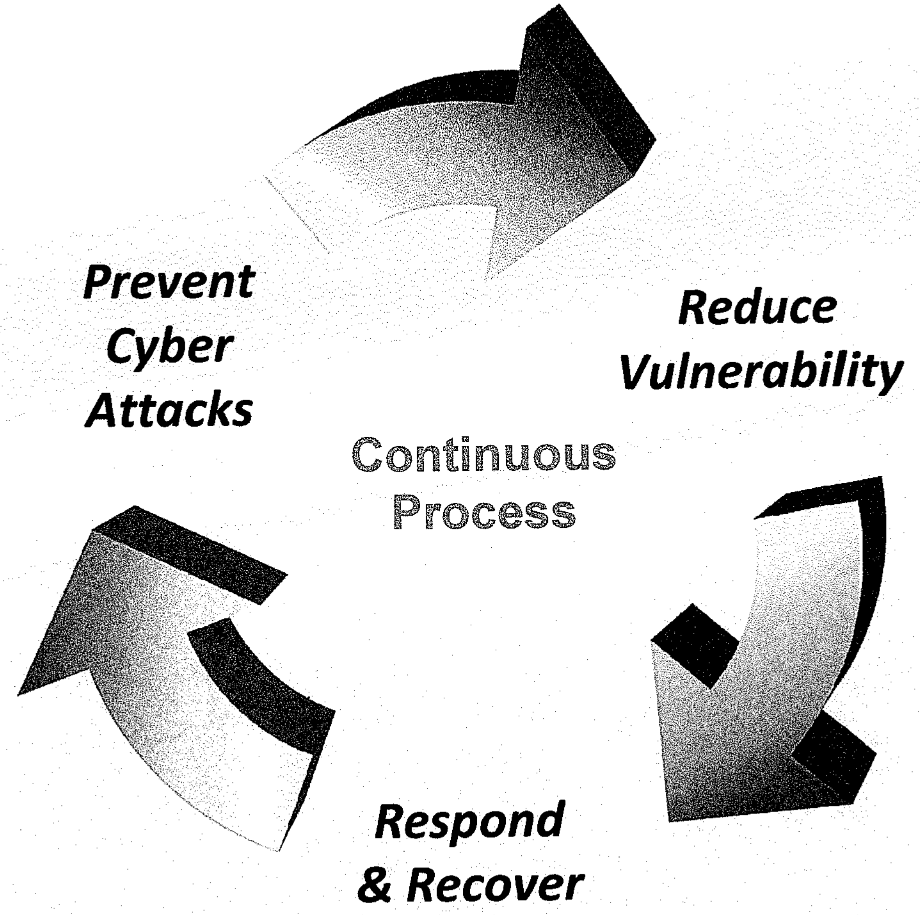
State Enterprise Security Plan
DEPT. OF INFORMATION RESOURCES

National Strategy for
Homeland Security (NSHS)
DEPT. OF HOMELAND SECURITY

The National Strategy to
Secure Cyberspace (NSSC)
WHITEHOUSE

State Enterprise Security Goals

- **Prevent cyber attacks** against Critical Infrastructure
- **Reduce vulnerability** to cyber attacks
- **Respond and Recover** to minimize the impact



Source: *State Enterprise Security Plan, 2007-2012*

Building State Response Capability

- Computer Security Incident Response Team Training
- Sentinel Project: CyberTerrorism Incident Handling, First Responder, Defense & Prevention courses

The SENTINEL Project
Free Cybersecurity Training Courses

- Act-Online Cyber Security Training (10 courses)
  - 500 Enrollments, over 300 completions

act online
www.act-online.net

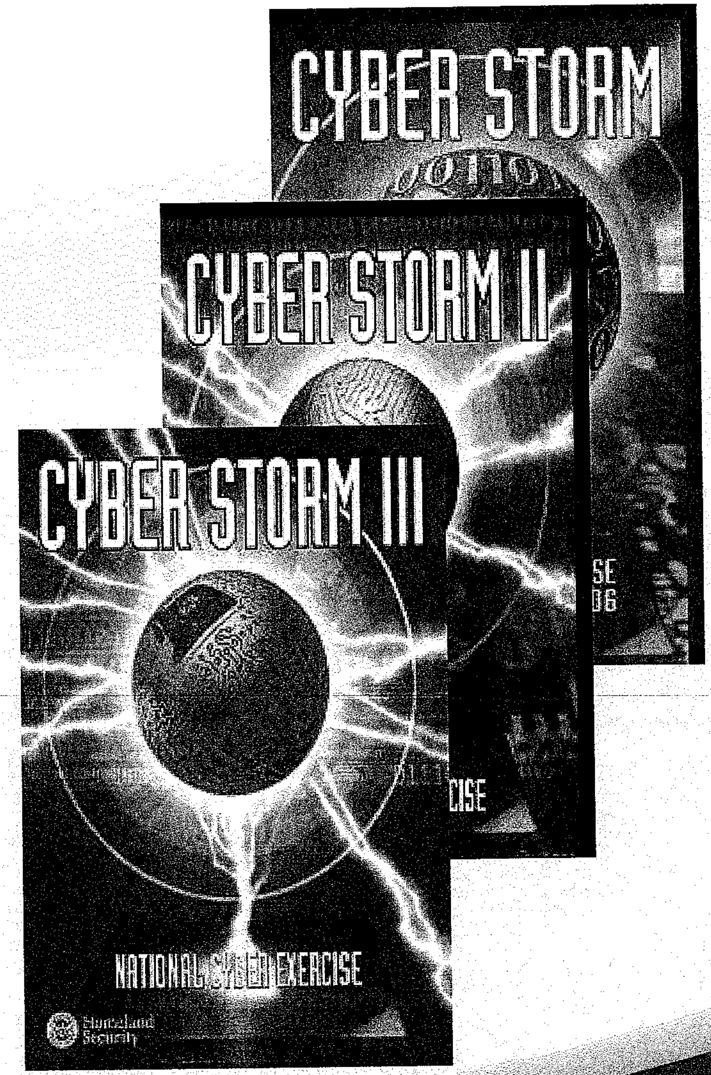
- UT San Antonio's CIAS training (Telecom Sec, Exercises)
- Annual DIR Information Security Forum

TEEX
TRAIN • SERVE • RESPOND

- 30+ events & 24k hours training provided FY08-09

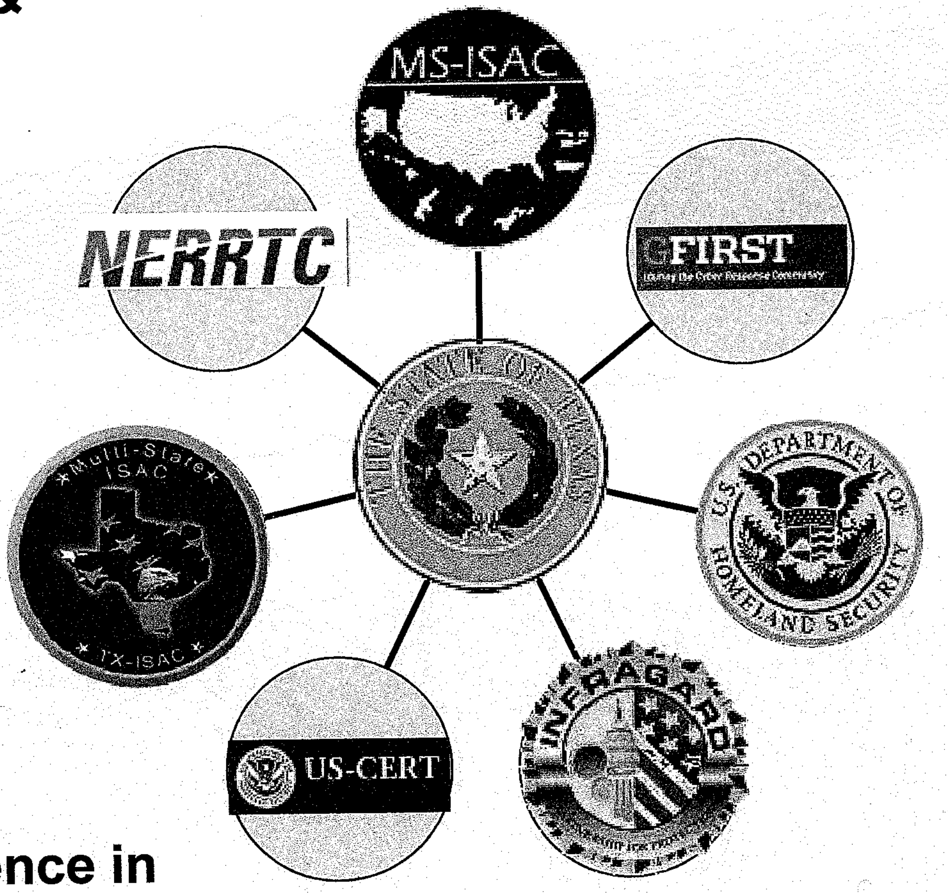
Cyber Storm: National Biennial Exercise Program

- Cyber Storm Series is a continuous learning and evaluation process
- Provides an opportunity for an intensive collective exercise of the cyber incident community
- Identifies significant areas for improvement and/or critical gaps in capabilities, processes, and procedures



Cyber Alerting and Information Sharing Partners

- Multi-State Information Sharing & Analysis Center
- Government Forum for Incident Response Teams
- US-CERT
- Infragard
- National Emergency Response and Rescue Training Center
- Governor's Homeland Security Council
- Texas Information Sharing & Analysis Center
- NSA National Centers of Excellence in Information Assurance


MS-ISAC
NERRTC
FIRST
Multi-State ISAC
TX-ISAC
U.S. Department of Homeland Security
US-CERT
Infragard