

**FUSION '05 :: NEBRASKA**

**Tuesday, November 15, 2005**

**Cyber Security –  
Now....More Than Ever!**

*Elayne Starkey  
Chief Technology Officer  
State of Delaware*



## **TODAY'S AGENDA**

- ✓ **The Cyber Security Threat:  
Why Worry?**
- ✓ **The Hacker's Lab**
- ✓ **Multi-State ISAC**
- ✓ **Enterprise-wide Cyber Security  
Program-Best Practices**
- ✓ **Steps to Success**



## Experts Warn U.S. Is at Risk for Cyberattacks

Industry insiders say an  
attack is likely within the next year,  
and say the government is not prepared.

Scarlet Pruitt,  
IDG News Service

**WARNING**  
OVER NEW TYPE OF  
COMPUTER VIRUS

Update: NASA  
investigating  
hacker theft of  
sensitive  
documents  
By DAN VERTON

## US fears al-Qaida hackers will Hit vital computer networks

Julian Berger in Washington

## Russian hacker breaks into US bank database

ComputerWire

# Hackers Attack Public, Private Sectors

By Dennis Fisher

## FBI Warns Of Hacker Attacks

By David Becker

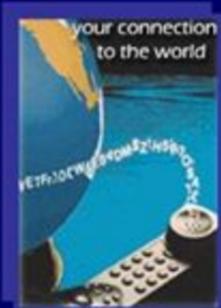
## DESPITE MORE SECURITY SPENDING INTERNET A MORE DANGEROUS PLACE

By ANICK JES DANUM - Associated Press



# The Interdependency between Information Systems and Critical Infrastructures

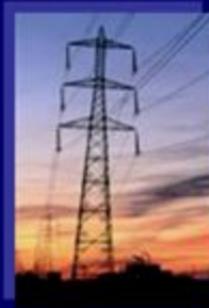
**Information & Communications**



**Transportation**



**Energy**



**Coordination**



**Emergency Services**



**Banking & Finance**



**Government**

# Citizens are demanding better, more cost effective and **SECURE** government services

- Digital Government that works
  - New, faster, easier ways to meet expanding needs of citizens
  - Facilitate collaboration to help businesses expand into new markets
- "One view of Government"
  - Go one place, one time for services
- Provide Better Services at Lower Cost
  - The Great Government Challenge... "Do More for Less"
- Increased Security and Privacy Demands
  - Maintaining trust will be essential
  - Expectations of "protection" extend to digital environments
  - Maintaining privacy while increasing services are often in conflict



# NASCIO Strategic Issues 2005

## • INFORMATION SECURITY

- IT Procurement Reform
- Privacy
- Interoperability and Integration
- Enterprise Architecture
- IT Governance and Services Reform
- Government Transformation and Innovation

# By The Numbers...

- General Internet attack trends are showing a **64%** annual rate of growth (Symantec)
- The average organization experiences **32** cyber-attacks per week (Checkpoint)
- The average measurable cost of a serious security incident in 2005 was approximately **\$1,000,000** (UK Dept of Trade & Industry)
- Identify theft related personal information is selling for **\$500-\$1000** per record (CFE Resource)
- Average of **80** new vulnerabilities per week !!

Friday November 11, 2005

# DAILY NEBRASKAN

**LEARN HOW TO WIN.**

HarperBusiness



**SCHOOL RELATIONSHIPS. CAREER.**

[Click Here](#)

Interact: [TheDirectory](#)

[Front Page](#) [News](#) [Sports](#) [Opinion](#) [Arts](#) [Extra](#) [About us](#) [Advertising](#) [DN Alumni](#) [Classifieds](#) [E-mail Lists](#) [DN Mall](#) [Archives](#)

Search News [options](#)

## CURRENT HIGHLIGHTS

### LAW & ORDER [\(1\)](#)

[IVAN LOVEGREN: Capitalism creates, oppresses lower class](#) [\(1\)](#)

[Ron Jovi brings clean, easygoing attitude to Qwest Center](#) [\(1\)](#)

[Finding the perfect dress](#) [\(1\)](#)

[Daily Nebraskan Staff & Contact Information](#) [\(1\)](#) 2

[Classified Ad Form](#)

[A Century of the Daily Nebraskan](#) [\(1\)](#) 2

## SECURITY BREACH IN NEBRASKA STATE GOVERNMENT

By Mark Media  
Staff Writer

Some **NEBRASKA state workers** may have had their salaries and other personal information compromised after someone gained unauthorized access to a state agency's computer.

The State has begun warning some current and former household workers that the state for whom they may have been accessed by an intruder's letter was someone that people of the breach and offering information about how to reduce the risk of identity theft.

Approximately 5,000 employees were affected. The database in question contained names, Social Security numbers and wages.

At this time **we do not know the intent of the intruder** or whether your personal information was accessed," Dale Morgan, chief information security officer of the EDD, said in the letter.

[News](#)

[Sports](#)

[CFA meets with UHC](#)

[Brandenburg ready for action](#)



**cornwear**

1 unique you.

3 unique cards.

Infinite possibilities.



## Security

## State agency warns of security breach

Last modified: February 13, 2004, 10:06 AM PST

By Ina Fried

Staff Writer, CNET News.com



PRINT



EMAIL



SAVE

**Some California workers may have had their salaries and other personal information compromised after someone gained unauthorized access to a state agency's computer.**

The **California Employment Development Department** has begun warning some current and former household workers that their information may have been accessed by an intruder, CNET News.com has learned. The agency sent a letter, dated Feb. 11, notifying people of the breach and offering information about how to reduce the risk of identity theft.



With In  
Centriq  
techno

Only

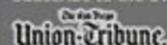
Order on  
shipping

GetUp to



- News
- Local News
- Opinion
- Business
- Sports
- Currents Weekend
- The Last Week
- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Weekly Sections
- Books
- Personal Tech
- Enlace
- Family
- Food
- Home
- Homescape
- Insight
- Night & Day
- Religion & Ethics
- Sunday Arts
- Travel
- Quest
- Wheels

Subscribe to the UT



Home Delivery  
from \$1.50 per week



# UCSD says computer server hit by hackers

## Confidential information on 380,000 compromised

By Eleanor Yang

STAFF WRITER

May 7, 2004

About 380,000 University of California San Diego students, alumni, faculty, employees and applicants had their confidential information compromised after hackers broke into a university server.

They infiltrated four computers that stored social security and driver license numbers in the university's business and financial services department. Although investigators are unaware of illegal use of the data, they are urging those affected to take steps to guard against identity theft.

"We have no evidence any of the (confidential) data was accessed," said Elazar Harel, UCSD's assistant vice chancellor for administrative computing and telecommunications. "Most likely it was not, but we can't say that for sure."

They say at least one of the computers was used as storage for a DVD movie, perhaps for illegal file-sharing.

A state law that went into effect in July requires that companies and state agencies contact people when their computerized personal data has been compromised. State officials said yesterday that UCSD's notification is

Advertisement

"We deeply regret that unauthorized intruders have broken into one of our computer networks, possibly compromising the personal information of students, staff, faculty and others,"

**380,000 records of personal data including names, social security numbers, and drivers license numbers.**

### Local featured jobs

**WAREHOUSE Export**

SAN DIEGO, CA  
7 ARGON CORPORATION

**ADMIN ASST/RECEPTIONIS**

FALLBROOK, CA  
CONSTRUCTION

**ACCOUNTING/ BILLING**

SAN DIEGO, CA  
Confidential

**Janitors and Floor Cleaners**

CHULA VISTA, CA  
Confidential

**HVAC Project Manager/Commercia**

SAN DIEGO, CA  
Pacific Rim Mechanics

**Hairstylist and Receptionist Positions**

SAN DIEGO, CA  
Confidential



miLoanHunt.com

GO

compare mortgage rates from several lenders

[▶ Previous Story](#)[▶ Next Story](#)SEARCH  
detnews.com

Go

Home Page  
Essentials  
Cyber Surveys  
Forums  
Photo Galleries  
Weather  
Horoscope  
Lottery  
Giveaways  
Crossword  
Advanced Search  
Contact Us

Autos

Autos Insider  
Drive  
-- Car Reviews  
-- Latest Deals  
-- Model Reports  
Joyrides

Thursday, July 15, 2004

## Hackers turn Arkansas government servers into al-Qaida video hub

By David McGuire / Washington Post

An Internet computer server operated by an Arkansas government agency was transformed last weekend into the online home of dozens of videos featuring Osama bin Laden, Islamic jihadist anthems and terrorist speeches.

State government officials removed the files from a computer operated by the Arkansas Highway and Transportation Department shortly after they were discovered, a government spokesman said. The case highlights an increasing trend of hackers hijacking vulnerable Web servers for the purpose of advocating radical political and terrorist ideologies.

- [▶ Comment on this story](#)
- [▶ Send this story to a friend](#)
- [▶ Get Home Delivery](#)



SEARCH

The Web  CNN.com

Search

Enhanced by: Google

- Home Page
- World
- U.S.
- World Business
- Technology**
- Science & Space
- Entertainment
- World Sport
- Travel
- Weather
- Special Reports
- ON TV
- What's on
- Business Traveller
- Global Office
- Music Room
- Talk Asia
- Services
- Languages

# TECHNOLOGY

## IRS warns taxpayers about identity theft e-mails

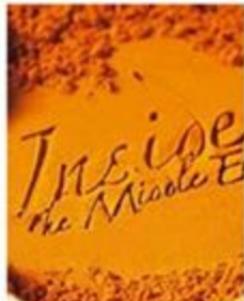
Saturday, May 1, 2004 Posted: 0137 GMT (0937 HKT)

WASHINGTON (AP) -- The Internal Revenue Service on Friday warned consumers about an identity theft operation that tries to elicit personal information from taxpayers by sending e-mails alleging they're the subject of a tax investigation.



advertisement

- [Question Of The Day](#)
- [Travel the World](#)
- [CNNarabic.com](#)
- [Sports Update](#)



# Same House....Multiple Doors



# How do Hackers find your unlocked doors?

## Scanning, Scanning and More Scanning

- Port Scanners

- Vulnerability Scanners

- Web Application Scanners

## Trial and Error

Attackers have unlimited amounts of time and resources

## Publish and Share

Attackers often find issues with sites and publish their techniques to obscure locations (chat rooms, foreign language hacker forums, etc.)





+tools&amp;btnG=Google+Search

[News](#) [Froogle](#) [Local](#) [more »](#)

Search

[Advanced Search](#)  
[Preferences](#)Results 1 - 10 of about 4,220,000 for **hack** tools with Safesearch on. (0.10 seconds)commonly used to **hack** computer

tools can be used to ...

[id](#) - [Similar pages](#)[ation and Internet Security Portal](#)

more than 6,03 GB of data -

...

[Similar pages](#)

## Tools

remote tools, adware, spyware,

ns **Hacker tools**, ...[ols.htm](#) - 21k - [Cached](#) - [Similar pages](#)

s part of the HP Calculator Archive.

ep 4, 2005 - [Cached](#) - [Similar pages](#)





# DEFCON

Welcome to the largest underground hacking event in the world.

## Community



dc forums  
[forum.defcon.org](http://forum.defcon.org)



dc groups  
Founded to bring people who cater to the same interests to share their knowledge.



mailing lists  
A listing of other hacker related & computer security mailing lists.



calendar of events  
Submit your upcoming cons and other hacker related events!

## Scene

1978 - 2005

In Memory of Josh Cohen,  
aka Pac-Bell

defcon 13

[post-DEFCON 13](#). Our biggest year ever. Thank you all for making the con a huge success.

## News

DEFCON 10 Audio & Video Re-encoded... includes new content such as the Awards Ceremony.

Red Herring (Feb 2005): DT

# DEFCON THIRTEEN

// THE LARGEST UNDERGROUND HACKING EVENT IN THE WORLD

DEFCON 13

Las Vegas, Nevada, July 29-31, 2005

\$80 USD CASH ONLY

Typical dress code: jeans and black t-shirts

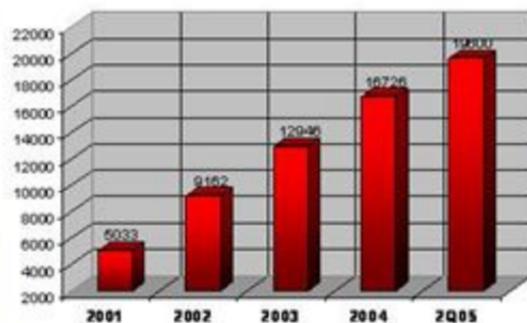
## Sample Seminars:

- Credit Cards: Everything You have Ever Wanted to Know
- Bypassing Authenticated Wireless Networks
- Protecting Hackers' Identities
- TCP/IP Drinking Game with Mudge
- Hacker Jeopardy XII - Fri and Sat night starting at 22:00
- Shmoo-Fu: Hacker Goo, Goofs, and Gear with the Shmoo

# Rapidly *increasing* threats and vulnerabilities

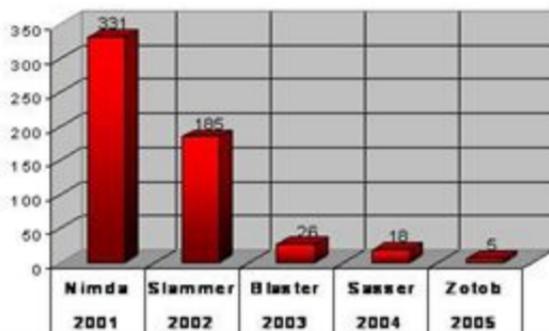
## Rapidly *decreasing* time to exploit

Cumulative Vulnerabilities Reported



CERT/CC

Days from Discovery to Exploit



CERT/CC, Microsoft, SANS

## No corresponding increase in IT resources

# Microsoft's August Security Bulletins

Released Tuesday August 9, 2005

## **CRITICAL**

- MS05-038 Cumulative Security Update for Internet Explorer
- MS05-039 Vulnerability in Plug and Play
- MS05-043 Vulnerability in Print Spooler Service

## **IMPORTANT**

- MS05-040 Vulnerability in Telephony Service
- MS05-041 Vulnerability in Remote Desktop Protocol

## **MODERATE**

- MS05-042 Vulnerabilities in Kerberos

This message was sent with High Importance.

From: Pelgrin, William (CSCIC) [mailto:William.Pelgrin@cscic.state.ny.us]  
 To:  
 Cc:  
 Subject: MS-ISAC Advisory - New MS Plug and Play Vulnerability Risk - High (UPDATED)

Sent: Fri 8/12/2005 12:36 PM

## Multi-State Information Sharing and Analysis Center Cyber Advisory

## MS-ISAC ADVISORY NUMBER:

2005-013-Updated

## DATE ISSUED:

August 9, 2005

August 12, 2005 Updated

## SUBJECT

New Vulnerability in Microsoft Plug and Play

## OVERVIEW:

A critical vulnerability exists in the Microsoft Plug and Play (PnP) service which allows an attacker to remotely execute arbitrary code on an affected system. The Plug and Play (PnP) service is used to simplify the installation of new hardware on most Windows-based operating systems. If an attacker successfully exploits this vulnerability, it will give the attacker complete control over the affected system. Exploit code was not publicly available at the time of our original advisory.

## August 12, UPDATED INFORMATION:

An exploit for this vulnerability has been made available to the public (See <http://downloads.securityfocus.com/vulnerabilities/exploits/Win2000-MS05-039.c>) and CSCIC has successfully tested it against a vulnerable host running Microsoft Windows 2000. This significantly increases the potential for this vulnerability to be actively exploited very soon so this patch should be tested and applied immediately if you are using Windows 2000. Microsoft Windows XP and Windows Server 2003, although vulnerable to this issue, require valid authentication credentials in order to be exploited therefore patching XP and 2003 systems is important but not as urgent.

## SYSTEMS AFFECTED

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Service Pack 2
- Microsoft Windows Server 2003 Service Pack 1

## RISK

## Government:

- Large and medium government entities: High
- Small government entities: High

## Businesses:

- Large and medium business entities: High
- Small business entities: High

## Home users: High

## DESCRIPTION

*...and 3 days later the exploit code is publicly available...*

Links

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail

Address <http://www.cnn.com/2005/TECH/internet/08/16/computer.worm/>

Pop-up blocked. To see this pop-up or additional options click here...

**CNN.com** WITH FREE YEALD Member Services International Edition | Netscape

MAKE CNN.com YOUR HOME PAGE

SEARCH THE WEB CNN.com SEARCH Powered by Y!oo! search

- Home Page
- World
- U.S.
- Weather
- Business at CNNMoney
- Sports at Slam
- Politics
- Law
- Technology**
- Science & Space
- Health
- Entertainment
- Travel
- Education
- Special Reports
- Video NOW FREE
- Autos with iStock.com

# TECHNOLOGY

## Worm strikes down Windows 2000 systems

Microsoft in 'emergency response' as worm reported on three continents

Wednesday, August 17, 2005. Posted: 11:02 a.m. EDT (15:02 GMT)

WASHINGTON (CNN) -- A fast-moving computer worm Tuesday attacked computer systems using Microsoft operating systems, shutting down computers in the United States, Germany and Asia.

Among those hit were offices on Capitol Hill, which is in the midst of August recess, and media organizations, including CNN, ABC and The New York Times. Caterpillar Inc., in Peoria, Illinois, reportedly also had problems.

A small number of computers in an administrative office at San Francisco International Airport also crashed, but they were not essential to the airport's operation, spokesman Mike McCarron said.



Search Jobs more jobs

Enter Keywords

Enter City ALL

careerbuilder.com SEARCH

IBM

ibm.com/ondemand

advertiser link: [what's this?](#)

**Save on All Your Calls with Vonage**

When looking for local regional and long distance calling, use Vonage to make... [www.vonage.com](http://www.vonage.com)

**MyCashNow - \$100 - \$1,500 Overnight**

Payday Loan Cash goes in your account overnight. Very low fees. Fast decisions.

*...and 5 days later the Zotob worm is released...*

Make phone calls through your high-speed internet connection.

**lingo**

SIGN UP NOW!

**SERVICES**

E-mail Newsletters

Your E-mail Alerts

RSS more

CNNtoGO

Contact Us

SEARCH

WEB CNN.com



**The Cavalry Arrives**  
 Armed troops storm into New Orleans; Bush tours disaster area  
 • Video: Frustration



**Shiites Rally**  
 Shiites rally in support of Iraq's new constitution and government; three GIs killed



**U.N. Official Indicted**  
 A Russian U.N. official indicted in U.S. in oil-for-food scandal

[EMAIL STORY](#)
[PRINTER FRIENDLY](#)
[FOXFAN CENTRAL](#)
**MORE U.S. & WORLD HEADLINES**

## Suspected Computer Worm Creators Arrested

Friday, August 26, 2005  
 Associated Press

**WASHINGTON —**  
 Authorities in Morocco and Turkey have arrested two people believed to be responsible for unleashing a computer worm that infected networks at U.S. companies and government agencies earlier this month, the FBI said Friday.

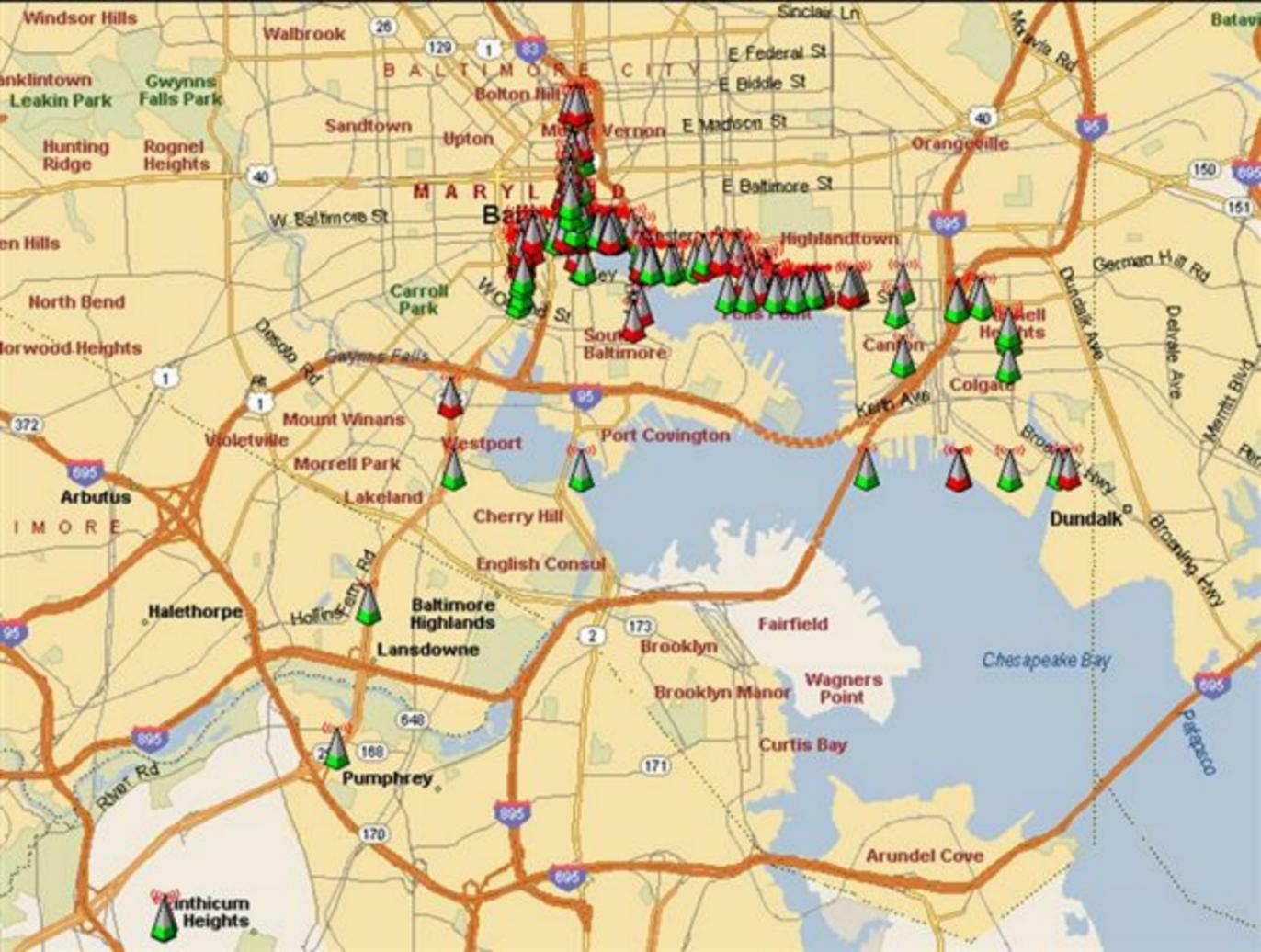
**STORIES**

- Variants of Computer Worm Strike Microsoft Systems
- Teen Confesses to Creating 'Sasser' Worm
- Web Worm Slows Google Searches
- 'Sasser' Worm Disrupts Asian Computer Networks

Faïd Essebar, 18, was arrested in Morocco, while Atilla Ekici, 21, was arrested in Turkey on Thursday, the FBI said. They will be prosecuted in those countries, the FBI said.

- Saddam's First Trial to Begin Oct. 19
- GI, Taliban Chief Killed in Afghanistan
- U.N. Offers Hurricane Disaster Assistance
- La. Justice System to Change After Katrina
- Australia, Japan Among Nations Offering Aid
- Officials: Draining City Will Take Weeks
- Russia Can't Guarantee Complete Security, Putin Tells Beslan Moms
- Nataliee Suspect to Be Freed in Aruba
- Missing Americans Found Dead in Canada

*...and 10 days later two arrests are made.*

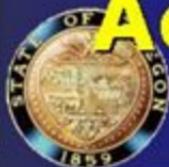


# SECURITY

**"Redoubling Our Efforts  
To Secure Our Nation's  
Critical Infrastructures"**



**Working Together**  
**Multi-State ISAC**  
**Across States...**



# MS-ISAC Background

- Recognizing the need for **collaboration and communication** between and among the states, the MS-ISAC was established in January 2003.
- The MS-ISAC began with the Northeast states, and quickly expanded.
- The MS-ISAC meets monthly via conference call and annually in person.
- Currently **all 50 states** and the **District of Columbia** participating.

# Objectives of the MS-ISAC

- **Disseminate early warnings of cyber security threats**
- **Share security incident information between Sectors**
- **Provide trending and other analysis for security planning**
- **Distribute current proven security practices and suggestions**

A graphic of the American flag with the stars and stripes, used as a background for the title text.

## Cooperation with National Partners

- White House Homeland Security Council
- U.S. Department of Homeland Security
  - National Cyber Security Division
  - Office of State and Local Government Coordination
- National Cyber Security Alliance

# Enterprise-wide Cyber Security Program

## Emerging Best Practices

- Treat Security Architecture as a PROGRAM, not a PROJECT
- Develop standards-based methodology (ISO, NIST, ITIL, COBIT, etc.)
- Establish Policies and assign critical effectiveness metrics
- Active and Aggressive Outreach Program
- Place CISO/CSO as high in organization as possible. Enable CISO/CSO to influence staff that are not direct reports
- Develop and manage a close working relationship with Department of Safety and Homeland Security
- Partner with Vendors
- Partner with a local university/college
- Don't wait until you have to REACT

# Steps to Success

- **Designate your primary Data Centers** as designated as one of the **State's most critical buildings**. This ensures accelerated emergency response, and around the clock police coverage when the threat level is raised.
- **Increase focus and attention on policies, procedures, standards** to help prepare for and respond to security concerns.
- **Partner** with Emergency Management and Law Enforcement.
- **Practice** a major cyber security breach
- Continually **remind** others of the threat: Governor's Office, Budget Office, and other key decision makers

35 MINUTES  
REMAINING

**Delaware's first-ever  
Cyber Security  
Tabletop Exercise  
September 13, 2005**





# Everyone's Challenges

- The need for security is growing as fast as our customer's needs for access and sharing of data
- Keeping our toolkit and defenses as advanced as the hackers'
- Staying current with vendors' security patches—requires planning and testing
- Continued education and awareness for the budget writers and other decision makers regarding the cyber security threat
- Find alternative funding sources
- Requires continued vigilance, continued investment of resources, and a concerted long-term effort

# IN CONCLUSION

Together, we are making significant progress in the protection of Government's information and communications assets,

**BUT**

there is more work to be done.  
This is a race with no finish line.



**YOU'VE BEEN  
WARNED**

# Questions?



Elayne M. Starkey  
Chief Technology Officer

---

State Of Delaware  
William Penn Building  
801 Silver Lake Boulevard  
Dover, DE 19904-2407

Voice: 302-739-9631  
Fax: 302-739-6251  
elayne.starkey@state.de.us  
SLC: D-410