

**WHERE WORLDS COLLIDE!**

A dramatic illustration of two planets colliding in space. On the left is a reddish-brown planet, and on the right is a blue and white planet. They are crashing together, creating a massive, bright orange and yellow explosion of fire and debris in the center. The background is a dark starry space.

## **Information Security and Risk Management**

February 18, 2008 | Washington, D.C.

**PRESENTERS:**

Sharon D. Nelson, Esq. & John W. Simek  
Sensei Enterprises, Inc.

**National Association of Regulatory  
Utility Commissioners**

# Protection of Critical Infrastructure Assets

- ❖ A hacker?
- ❖ A terrorist?
- ❖ A criminal?
- ❖ A foreign country's agent?



From the headlines

# CIA: Hackers to Blame for Power Outages!



# January 18, 2008

- ❖ CIA senior analyst Tom Donahue
- ❖ Reported at a SANS Process Control Security Summit
- ❖ Multiple areas outside the U.S. attacked
- ❖ Power equipment disrupted – multiple cities went black
- ❖ Had Internet access to computers controlling equipment
- ❖ Extortion demands followed
- ❖ Insider information suspected, not confirmed
- ❖ CIA debated release of this info extensively



# A little history

- ❖ The year is 2000
- ❖ The place is Australia
- ❖ Disgruntled former computer worker
- ❖ Hacked into a sewage control system
- ❖ Flooded parks, rivers and a hotel with a million gallons of raw sewage.



# A little history

- ❖ The year is 2003
- ❖ Slammer virus
- ❖ Disabled a safety monitoring system
- ❖ A T1 line bypassed the plant's firewall
- ❖ At an inactive Ohio nuclear plant
- ❖ No harm done . . . . fortunately



# Nuclear Plant Security????

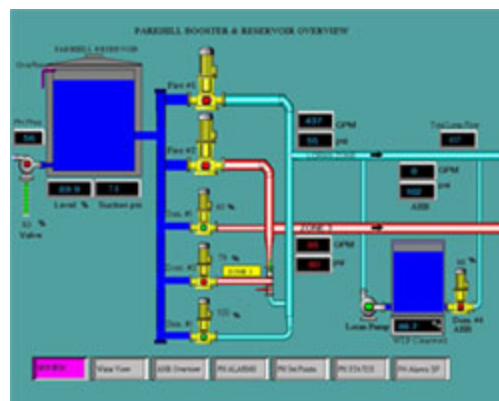


# SCADA



# Supervisory Control and Data Acquisition

- ❖ Specialized electronic equipment that operates power, water and chemical plants
- ❖ Increasingly connected to the Internet



# The Aurora Generator Test



# The Aurora Generator Test

- ❖ Conducted in March of 2007
- ❖ By Idaho National Laboratory
- ❖ Found a critical vulnerability in SCADA systems
- ❖ Homeland Security produced a video for government use
- ❖ Simulated breach by hackers
- ❖ Produced shuddering and smoking in a \$1 million diesel electric generator which then stopped functioning
- ❖ 2002 – U.S. government knew al Qaeda was interested in SCADA systems

AP Photo of test

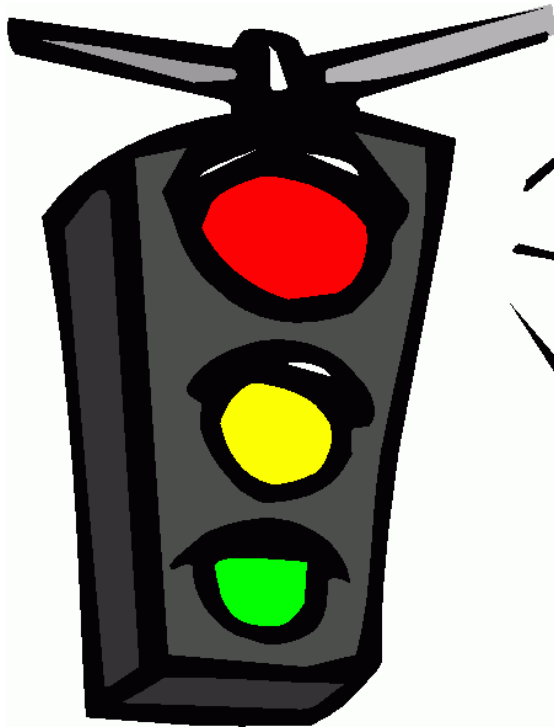


# How do we know about the Aurora test?

- ❖ Moronic Homeland Security employee presented the tape to a conference
- ❖ It took the A.P. six months of dogged pursuit to get a copy

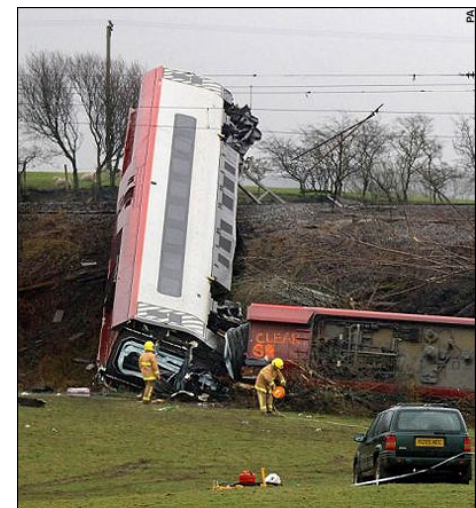


# Still another incident



- ❖ Vancouver, Canada
- ❖ September 27, 2007
- ❖ Civic employees' union had been picketing for 71 days
- ❖ City's central computer system was hacked
- ❖ Computer's clock was reset by 7 hours
- ❖ Traffic control signals went to night mode, with short intervals and traffic was hopelessly snarled

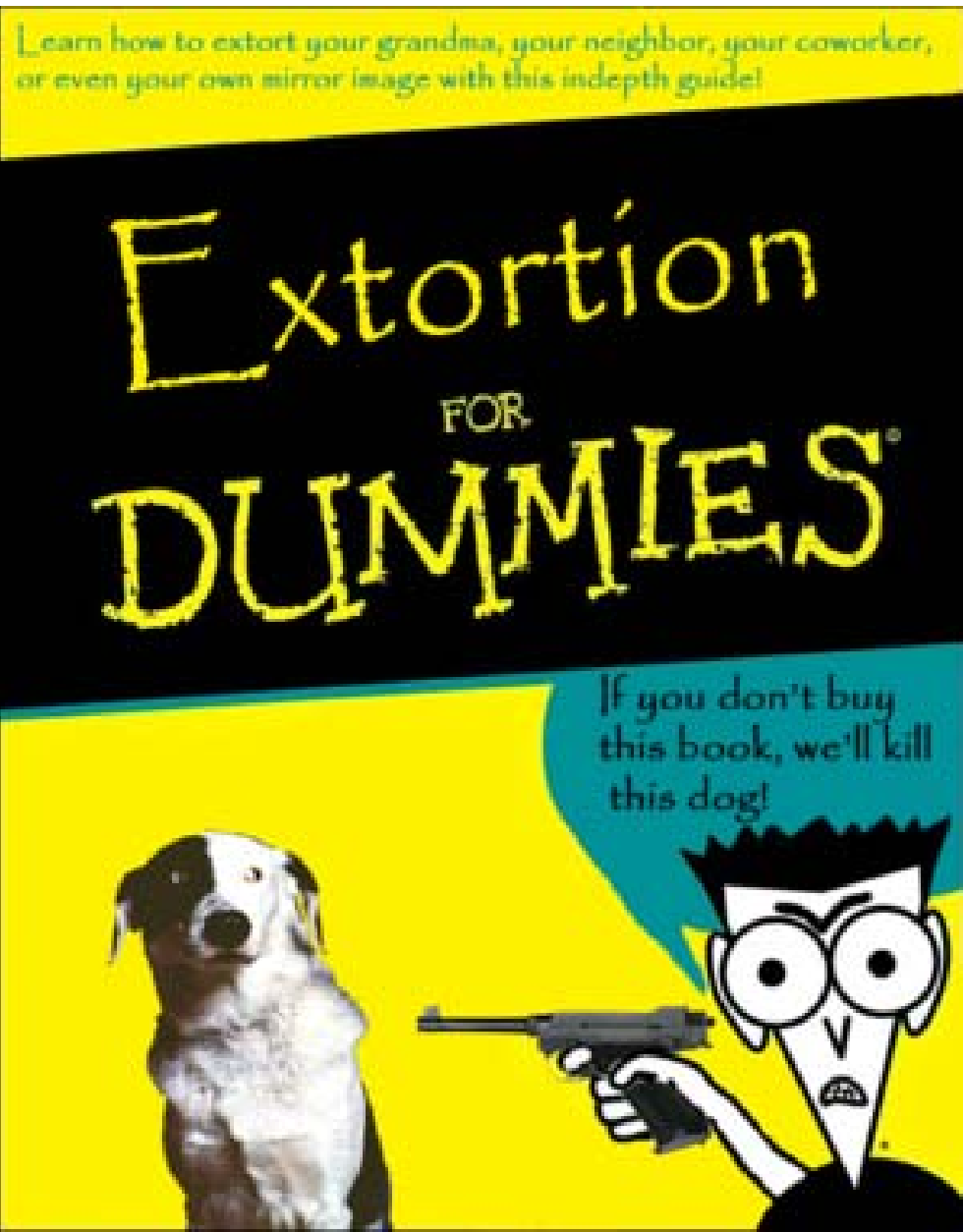
January 11/08 story out of Poland is my favorite. *"A Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailling four vehicles in the process. Twelve people were injured in one of the incidents. The 14-year-old modified a TV remote control so that it could be used to change track points..."* Described as an electronics buff and an exemplary student, the lad had notebooks full of observations made of the tram system. In other words he picked his target, did his recon, and then modified a simple household device which gave him control over a public utility.



# Cyberextortion

- ❖ Who at utility companies is trained for this?
- ❖ Why, oh why, are all computers necessarily connected to the Internet?
- ❖ Why are so many SCADA systems customized, which increases their vulnerability?

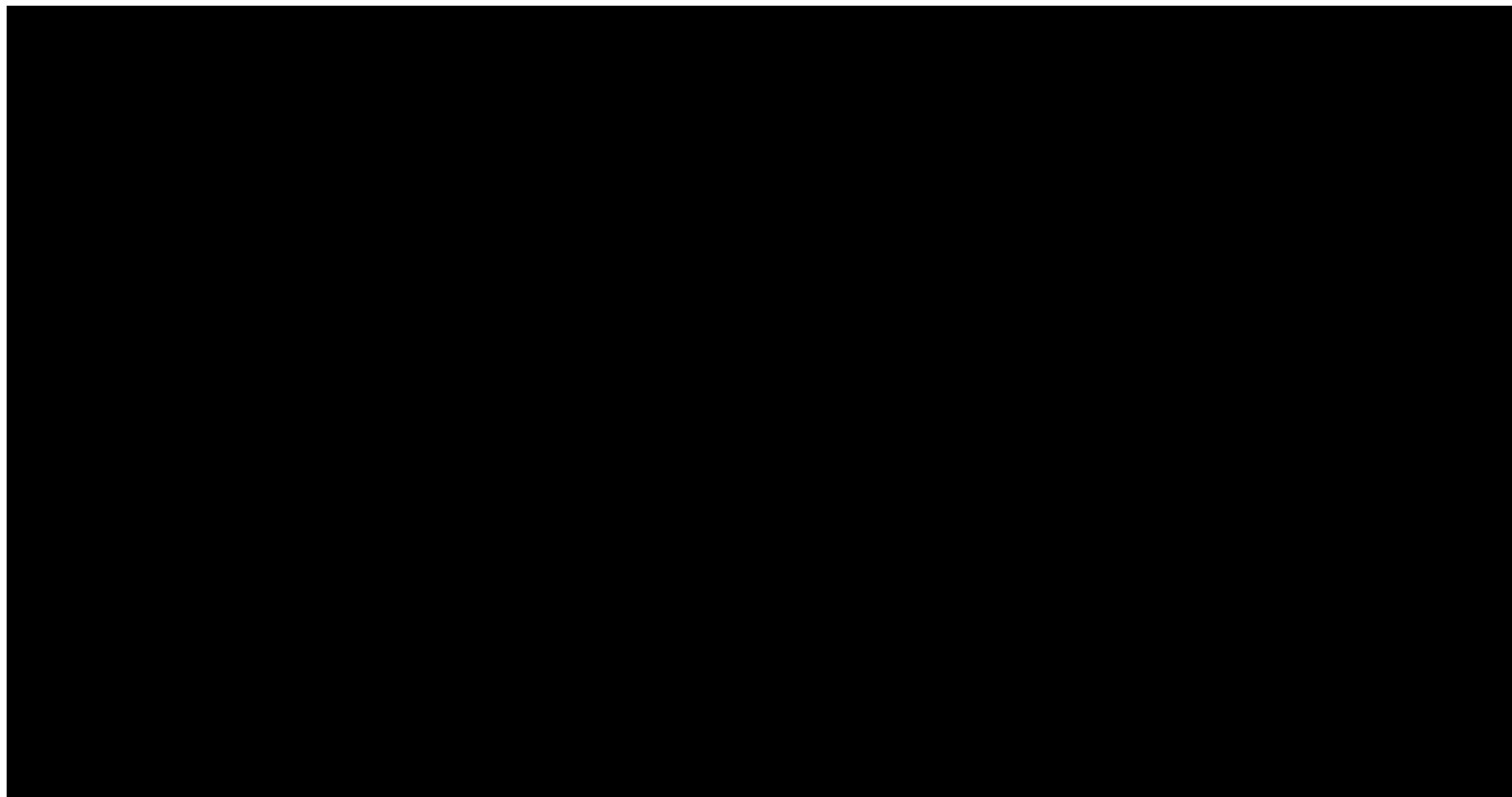




# The Lights of New York



# Who turned the lights out?



# Tip of the hat to Eric Byres, SCADA Security Specialist



# What are critical infrastructures?

- ❖ Infrastructure systems, for which continuity is so important that loss, significant interruption or degradation of service would have grave social consequences



# What are critical infrastructures?

- ❖ Power generation and distribution
- ❖ Oil and gas refining and distribution
- ❖ Water and waste systems
- ❖ Chemical processing and transport
- ❖ Manufacturing
- ❖ Telecommunications
- ❖ Banking
- ❖ Almost all controlled by a web of dedicated computers, a SCADA system



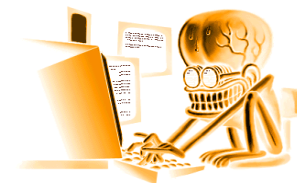
# What is the Industrial Security Incident Database (ISID)?

- ❖ ISID tracks network cyber incidents that impact industrial and SCADA operation
- ❖ Both malicious and accidental
- ❖ A huge upswing in 2001
- ❖ 1982-2001 – Incidents almost all internally driven
  - Accidental
  - Inappropriate employee activity
  - Disgruntled employee



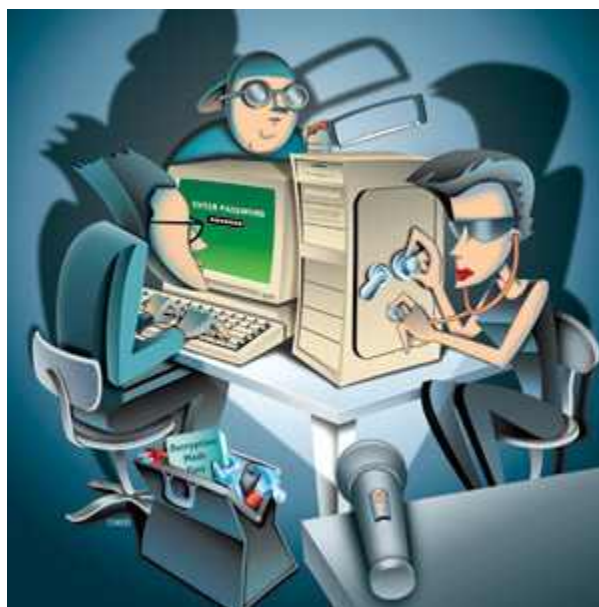
# Types of incidents 2002-forward

- ❖ Most incidents are externally driven
  - Virus/Trojan/Worm
  - System penetration
  - Denial of service
  - Sabotage
- ❖ Before 2002, only 27% of incidents were external
- ❖ After 2002, 61% of incidents were external
- ❖ Accidental incidents have grown too:
  - Poor design of products
  - Poor design of systems



# Report from SecureWorks

- ❖ October 2007
- ❖ 90% increase in the number of hacker attacks on utilities
- ❖ Average of 93 attack attempts each day



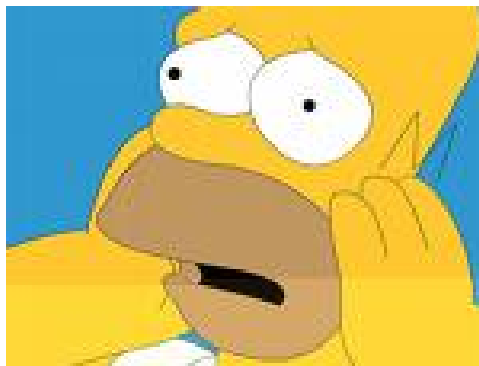
# Security Quality Assurance Testing

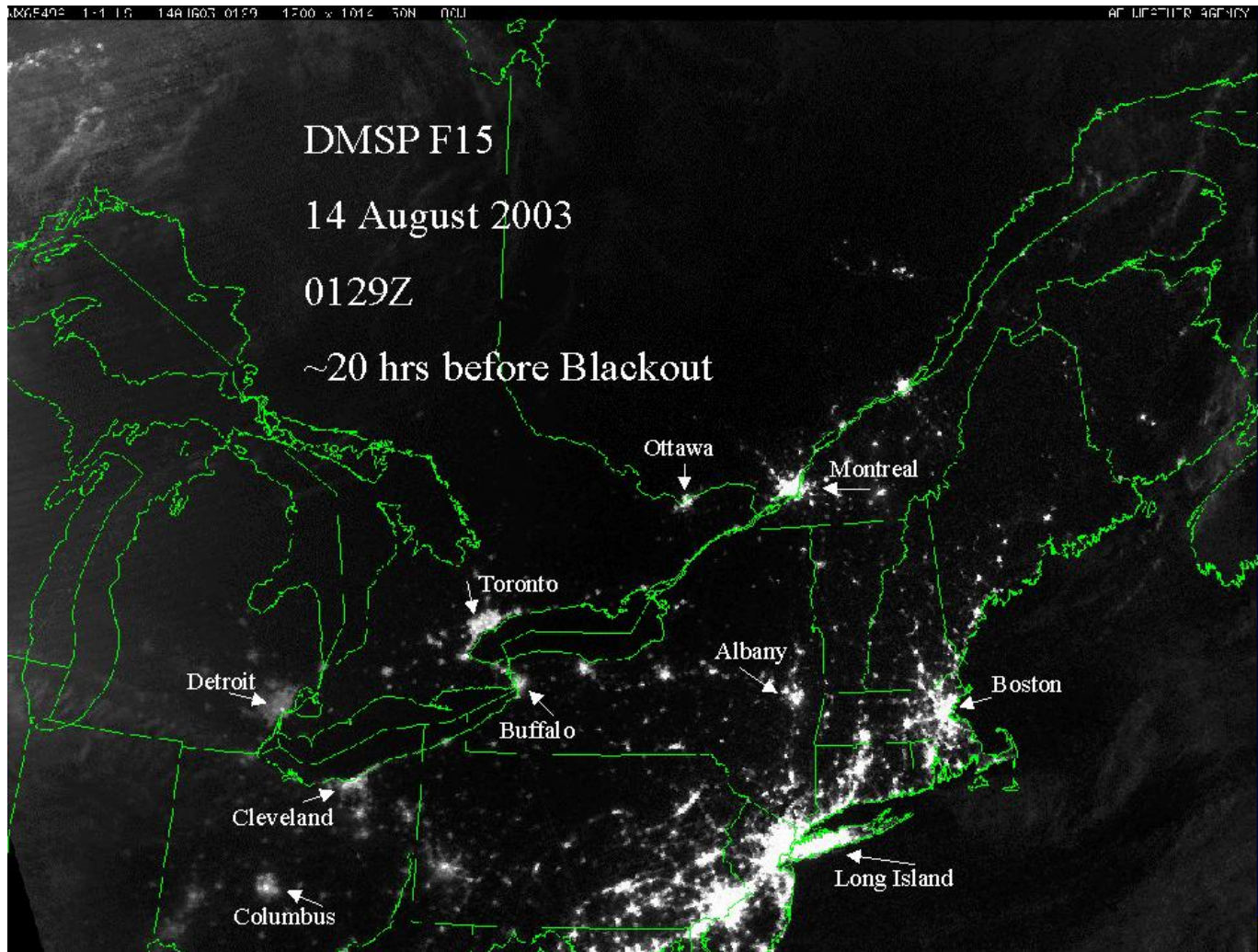
- ❖ Need to understand what products and devices actually do before they are implemented
- ❖ Test for vulnerabilities using known flaws
- ❖ Will it hold up under DoS attack?
- ❖ Is the device secure for buffer overflow?
- ❖ Fuzz testing: Direct pseudo-randomly created data sets to uncover unexpected behavior

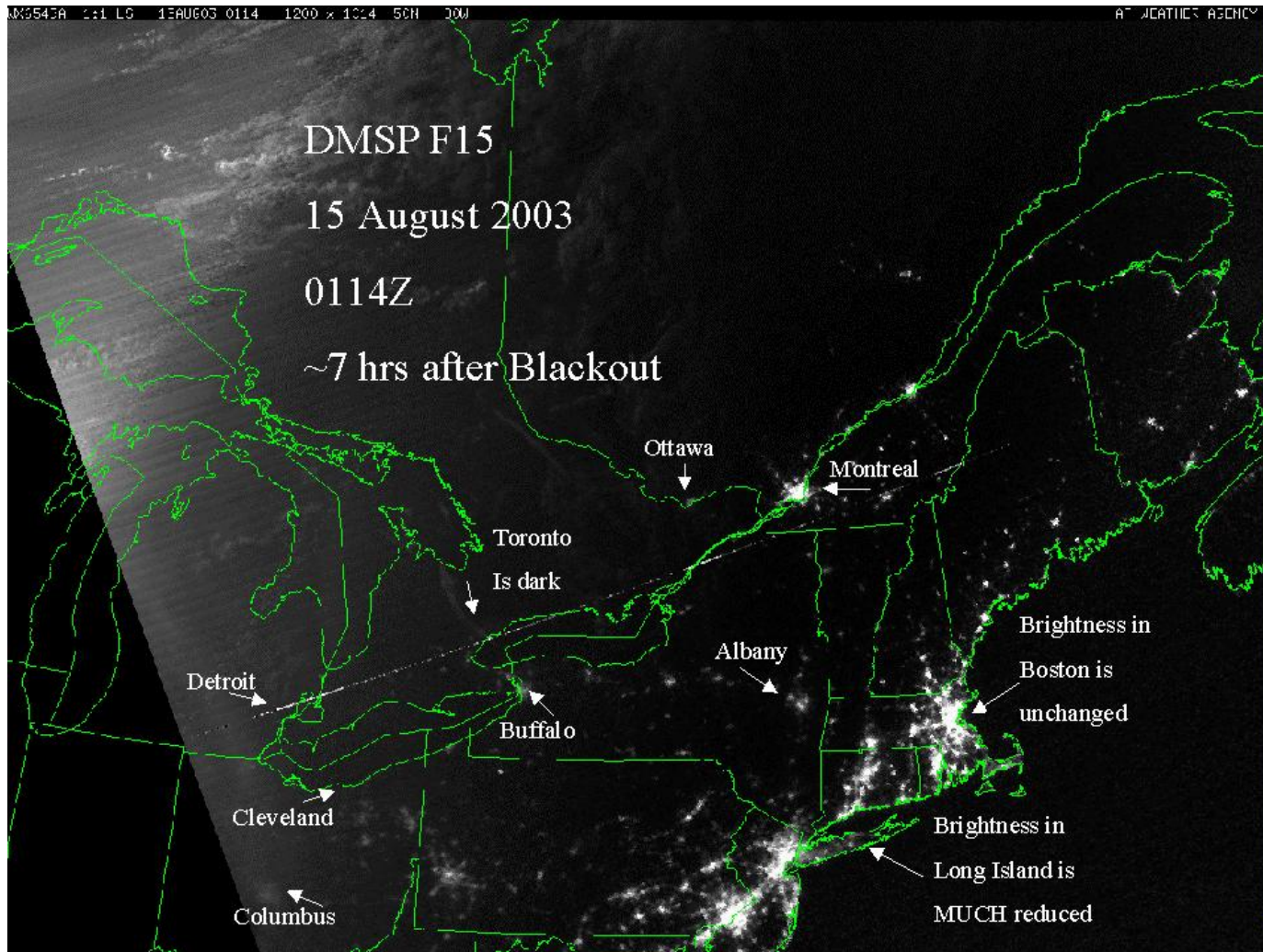


# The great northeastern blackout of 2003

- ❖ The blackout was caused by a flaw in widely-deployed General Electric management system.
- ❖ It took weeks of pouring through code to find it
- ❖ Operators did not know they were operating without alarms
- ❖ Electricity blackout affected 50 million people in eight states and Canada







# Federal Energy Regulatory Commission (FERC)

- ❖ January 17, 2008
- ❖ Eight new mandatory critical infrastructure protection (CIP) reliability standards were adopted
- ❖ To protect the national bulk power system
- ❖ Developed by the North American Electric Reliability Corporation (NERC), which FERC has designated as the electric reliability organization (ERO)



# New CIP standards

- ❖ Critical cyber asset identification
- ❖ Security management controls
- ❖ Personnel and training
- ❖ Electronic security perimeters
- ❖ Physical security of critical cyber assets
- ❖ Systems security management
- ❖ Incident reporting and response planning
- ❖ Recovery plans for critical cyber assets



# Why it matters

- ❖ According to experts, if one third of the country lost power for 3 months, the price tag would be \$700 billion
- ❖ The equivalent of 50 mega-hurricanes striking at once



Hurricane Opal – 1955,  
Alabama

# Government gathering, protecting, and using personal information

- ❖ From the security standpoint, not much has changed since we were last here
- ❖ However, there is one major development which we see rippling across government agencies



# Records Management

- ❖ Agencies which never had a policy are creating one
- ❖ Agencies which have policies are finally enforcing them
- ❖ They are also updating them
- ❖ You cannot protect data which is unclassified



# When we moved to the electronic world

- ❖ We took all the junk with us
- ❖ As we move to bigger servers, we continue to move the garbage onto larger hard drives
- ❖ Most organizations have no idea what they have
- ❖ Worse yet, many let records management be done by humans, and yet don't enforce compliance



# Monitoring compliance is key



# Proper records management

- ❖ There are many systems – hire a pro, don't do this internally
- ❖ Most provide a “janitorial” function, e.g. data is deleted within “X” days unless “tagged” and saved



# Tagging is very customized

- ❖ HIPAA data
- ❖ Core company documents
- ❖ Data to be held under a “litigation hold”
- ❖ Sarbanes-Oxley data
- ❖ Open project data
- ❖ Systems are complex, and yet must be made user friendly



# Dangerous legacy data

- ❖ Should be searched for problematic items
- ❖ Social security numbers
- ❖ Addresses
- ❖ Birth dates,
- ❖ Medical information
- ❖ Information about minors
- ❖ Criminal record information
- ❖ Credit card information
- ❖ This data (and current data) should be secured going forward



# Access control

- ❖ Perhaps the most critical internal element
- ❖ Who needs access?
- ❖ Log the access
- ❖ Track the activity
- ❖ Have alert systems in place
- ❖ Review access control at least annually
- ❖ Employee termination
- ❖ Change in internal status



# Without records management, you cannot be ready for e-discovery

How effective are your current discovery/e-discovery processes at your organization?

