INFORMATION SECURITY DECISIONS

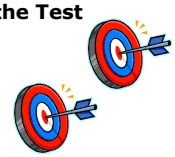
Hosted by

SLEEPING BETTER IN SEATTLE

Cyber Incident Response Put to the Test

Kirk Bailey, CISSP, CISM
CISO – City of Seattle

Ernie Hayden, CISSP
CISO – Port of Seattle



INFORMATION SECURITY DECISIONS

Hosted by

AGENDA

- INTRODUCE
  - THE CITY OF SEATTLE (Kirk's Stuff)
  - THE PORT OF SEATTLE (Ernie's Stuff)
- A HISTORY OF EXERCISES
  - ALKI
  - TOPOFF2
  - LIVEWIRE
  - BLUE CASCADES II
- SOME LESSONS LEARNED YOU CAN USE

INFORMATION SECURITY DECISIONS

Hosted by

"The views and opinions that I express here today are my own and may not be, in whole or in part, those of my employer, the City of Seattle…and for that matter, anybody else either!"

INFORMATION SECURITY DECISIONS

Hosted by

"The views and opinions that I express here today are my own and may not be, in whole or in part, those of my employer, the ~~City of Seattle~~...and for that matter, anybody else either!"

DITTO

Port of Seattle

INFORMATION SECURITY DECISIONS

Hosted by

City of Seattle

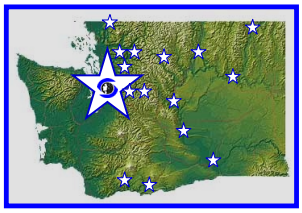
MY OFFICE ...a room with a very different view

Kirk Bailey
CISO, City of Seattle

INFORMATION SECURITY DECISIONS

Hosted by

City of Seattle
www.cityofseattle.net




INFORMATION SECURITY DECISIONS
Hosted by
SearchSecurity.com
Seattle Public Utilities
SEATTLE POLICE
Seattle Fire Department

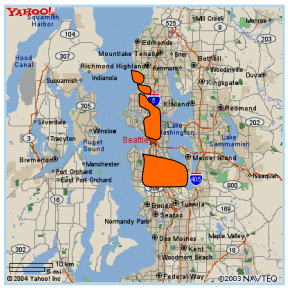

INFORMATION SECURITY DECISIONS
Hosted by
SearchSecurity.com
Port of Seattle


INFORMATION SECURITY DECISIONS
Hosted by
SearchSecurity.com
A Diverse Port

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

"City" of the Port of Seattle



- Multifaceted public agency
- Generates 165,000 jobs in region
- $5.5B payroll
- Revenue > $12B
- State & local tax generation >$660M
- Airport, seaport, fishing terminal, parks & recreation
- Police, fire and EMS services

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Infrastructure interdependencies

- Utilities
  - Power: Seattle City Light and Puget Sound Energy
  - Steam heat: Seattle Steam (Pier 66)
  - Gas: Puget Sound Energy
  - Telephone/Internet: Qwest, AT&T (Cell), NexTel (Cell), Verizon (Cell)
  - Water: Seattle public utilities & local water districts
  - Airport fuel transport: olympic pipeline
- Information Systems (servers, networks, 2000+ desktops)
- Railroads (BNSF, Union Pacific)
- Highways (I-5, I-90)
- Viaduct
- Banking / Finance

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

The big combined cyber picture

- 13,000+ Desktops and laptops
- 2,500+ Servers
- 1500+ Network peripherals (printers, fax, etc)
- 4,500+ Radios (all types)
- 3,000? PDAs (nobody knows)
- 18,000+ Telephones (desk and cell)
- Huge fiber and cable infrastructure (across state)

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Infrastructure interrelationships

- **Power**
- **Sewer**
- **Water**
- **Telecom**
- **800 MHz**
- **Transportation**
- **Cross Public Safety – Fire, Police, EMS**

- **Summary = We are all one!**

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

PHYSICAL THREATS

- Airport events
  - **Hijacking / hostage events**
  - **Crash – intentional or accidental**
- Railroad events
  - **Spills, stalls, derails**
- Container events
  - **Explosions, spills, suspicious cargo**
- Highway events
  - **Bridge destruction, tunnel destruction**
- Dams / locks **– destruction or damage**
- Earthquake / volcano / flooding

INFORMATION SECURITY DECISIONS

Hosted by

SEATTLE RANKS HIGH AS A TARGET
INSURANCE SERVICES OFFICE (NEW JERSEY)

Terrorism Risk Insurance Act of 2002
Indemnification for insurance companies for losses due to terrorism

1ST TIER (100X MORE LIKELY TO BE ATTACKED):
New York, Washington DC, San Francisco, Chicago

2nd TIER (20X MORE LIKELY TO BE ATTACKED):
Seattle, Los Angeles, Houston, Philadelphia, Boston

Tons of criteria including: geographical location, economic importance, accessibility as target (port city), iconic buildings and businesses, infrastructure sites, sports venues, intelligence indicators, and "gut feel."

INFORMATION SECURITY DECISIONS

Hosted by

Cyber-based Terrorist Threats:
Analysis for
The City of Seattle, and
The State of Washington

Confidential
(Disclosure Protection Provided under WA State RCWs)

Presented by: Kirk C. Bailey, CISSP, CISM
CISO, City of Seattle

INFORMATION SECURITY DECISIONS

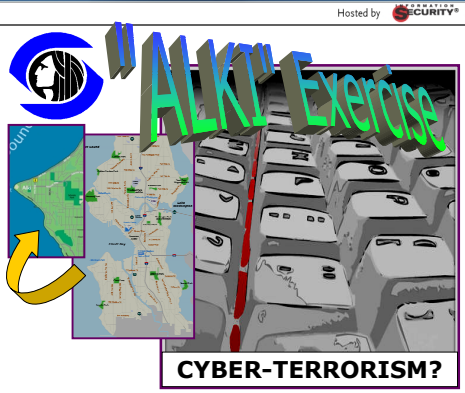
Hosted by

TABLETOP EXERCISES UNDERSCORE CRITICALITY OF CYBER-ISSUES

- **Vulnerability exercise**
  - **City of Seattle's "ALKI"**
- **International exercises – US / Canada**
  - **TopOff2**
  - **Livewire**
  - **BlueCascades II**

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com



CYBER-TERRORISM?

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

ALKI:
A VULNERABILITY ASSESSMENT EXERCISE

TABLETOP STYLE OF EXERCISE

FOCUS: "CYBER-TERRORISM"
AND OTHER ELECTRONIC THREATS

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

PARTICIPANTS

Hosted by…
City of Seattle &
SPD Emergency Preparedness Bureau

- **In collaboration with…**
the AGORA

- **From City of Seattle…**
DoIT, SPU, City Light, SDoT, Library,
SPD, SFD, EOC

- ***From Other Agencies…***
DoD, White House, DoE, etc.

INFORMATION SECURITY DECISIONS

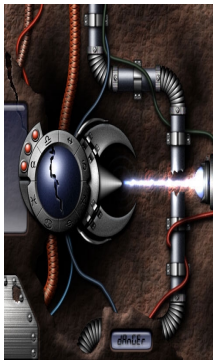
Hosted by

OBJECTIVE: ANSWERS TO THESE QUESTIONS…

- *What are the city's technical vulnerabilities?*
- *How might they be exploited?*
- *Are there any early warning signals?*
- *Are there any "low-hanging fruit" for mitigation?*
- *What about long-term mitigation?*

INFORMATION SECURITY DECISIONS

Hosted by



4 TEAMS:

1. *Long dwell*
2. *Short dwell*
3. *Trust team*
4. *Kill team*

INFORMATION SECURITY DECISIONS

Hosted by

Results from Alki exercise

- **Consensus findings**
- **Ranking of key targets**
- **Remediation recommendations**
  - **Governance**
  - **Policies & procedures**
  - **Training & education**
  - **Tactical – technical**
  - **Strategic - technical**

INFORMATION SECURITY DECISIONS

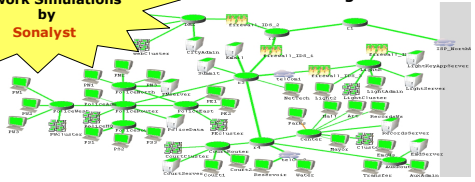
Hosted by SearchSecurity.com

Topoff2 CyberEx

May 6-7, 2003
Washington State Emergency Operations Center
Camp Murray, Washington

Designed and Controlled by:
Institute for Security Technology Studies (ISTS), Dartmouth College

Electronic Gaming Network Simulations by Sonalyst



INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

PARTICIPANTS

Government Players:

- City of Seattle
- King County
- State of Washington (DIS, EMD, DOT)

Supporting and Observing

- University of Washington
- Microsoft
- Boeing
- Qwest
- Seattle Joint Task Anti-Terrorism Task Force
- DHS (National Communications Systems)

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Designed to test incident response capabilities to a series of "force-multiplier" cyber-attack

Included 3 scenarios or vignettes:

(1) normal day at the office, with "normal" network and computer problems;

(2) an escalating series of events - computer and network problems which might be preliminary symptoms of a directed cyber-attack; and

(3) a major cyber-attack on participants' computer networks, coupled with a weapons of mass destruct (WMD) attack – a radioactive detonation device (RDD) terrorist bomb exploding in Seattle.

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Lessons learned and benefits:

- Top official awareness of cyber-related issues
- The value of delegated command and control
- Training and education needs identified
- The value of strategic and tactical network architecture
- Clearer understanding of cyber-threat spectrum
- The value of a trusted network neighborhood

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

National cybersecurity discovery event

LIVEWIRE

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Livewire purpose & focus

- Livewire was one component of an ongoing discovery process designed to provide DHS with input as it considers what a mature National Cyberspace Security Response System should look like.
- A primary goal of Livewire was to foster trusted relationships between differing organizations that might be part of this system.
- The discovery event provided a risk-free environment in which private-sector organizations practiced communicating and coordinating with their government counterparts

LIVEWIRE

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Livewire objectives

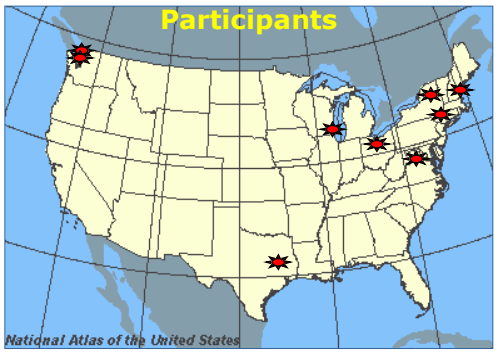
- Foster relationships between public and private sector organizations
- Help define and practice intra- and inter-organizational communications, coordination, and response decision-making
- Identify authority gaps and overlaps
- Validate large-scale, distributed, cross-sector cyber security exercises

Type of event: Actual Network Interface / Exchange

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

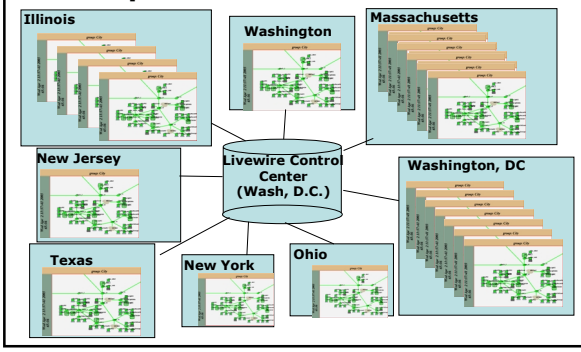
Participants



INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Participants



INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Event / scenario

- Time: Fall 2004
- Recent increase in cyber activity (significant)
- Source unknown – libraries, schools, foreign computers
- Intelligence points to terrorist intentions (since 2002)
- National intelligence focus on nation states of RED, BLACK, and PURPLE – referred to as the "Rainbow Trio"
- Since the 80s – these countries have ramped up cyber
- WMD issue between US and Trio – saber rattling, threats of military action, increased trade restrictions
- Ties between Trio and terrorists

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Livewire questions

- Who is in charge when cyber attack occurs?
- What is the Federal role in cyber defense?
- What is the appropriate response to a cyber attack?
- What are the economic impacts of a cyber attack?

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Blue Cascades II

King County

Pacific NorthWest Economic Region

PUGET SOUND ENERGY

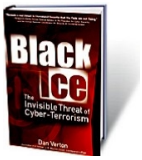
TransCanada
In business to deliver

Microsoft

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Blue Cascades II



- Focus on a cyber terrorism event followed event
- Blue Cascades II was follow-on to Blue Cascades I held in 2002
  - Dan Verton's Book Black Ice covers much of Blue Cascades I results
  - Blue Cascades I centered on physical attacks & disruptions
- Infrastructure interdependencies tabletop exercise

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Participants

- Sponsors:
  - Northwest Partnership for Regional Infrastructure Security
  - Pacific NorthWest Economic Region (PNWER)
  - King County
  - Microsoft
  - Puget Sound Energy
  - TransCanada
- Other players
  - Over 200 participants
  - DHS, CERT
  - DoD
  - Medical/hospitals
  - Public safety
  - Logistics companies
  - Canadian government players

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Objectives

- Raise awareness of interconnections among the region's critical infrastructures and organizations and associated vulnerabilities.
- Focus on attacks that disrupted business practices and operations of infrastructures and organizations, including critical telecommunications and electric power assets.

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Teams

- Scenario design team
- Tabletop segregation
  - Separate into critical infrastructures
    - Energy / electric power / gas
    - Government
    - Public safety – fire
    - Public safety - police
    - Medical
  - Independent evaluators
- Lessons learned team

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Results

- Large number of findings and recommendations
  - Participants
  - Independent evaluators
- Key Areas:
  - Understanding interdependencies and cyber threats and disruptions
  - Cooperation and coordination
  - Communications and information sharing
  - Incident management
  - Resource management
  - Public information and education
- Example: Regional Cyber Security Council (in infancy)

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Cyber exercise lessons learned...

Ideas to help you

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Lessons learned – What you can do

1. Don't worry about developing a complex plan – simple will work - just let everyone's imagination run free
2. Consider your focus on only cyber versus a combined cyber – physical attack – you'll be surprised at what you can learn
3. Tabletops are very effective – you don't need active, hardwired networks to play
4. Don't be afraid to ask others to play – you'll be surprise who's interested in helping
5. Consider non-disclosure agreements for you and the region's protection

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Lessons learned – What you can do (2)

6. Use a Facilitator to Drive the Discussions and Provide the "Injects"
7. Establish a Scenario Team to "Build" the Primary Event and Collect Foundational Materials
8. Cross-Group Your Teams – Let the Technical and Non-Technical Work Together to Improve Communications and Broaden the Perspectives
9. Collect Recommendations – Before, During and After the Exercise – Take Advantage of Each Idea
10. Don't Be Afraid to Try – Small is OK as well as the Giant Exercises

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

References

- **Blue Cascades II**
  - http://pnwer.org/pris/BCII_files/BCII%20Executive%20Summary.pdf
- **TopOff 2**
  - http://www.dhs.gov/interweb/assetlibrary/T2_Report_Final_Public.doc

INFORMATION SECURITY DECISIONS

Hosted by

INFORMATION SECURITY DECISIONS

Hosted by

Contact information

Ernie Hayden, CISSP
CISO
Port of Seattle
2711 Alaskan Way
Seattle, WA 98121
206-728-3460
Hayden.e@portseattle.org

Kirk Bailey, CISSP CISM
CISO
City of Seattle
Suite 2700
700 Fifth Avenue
Seattle, WA 98104
206-684-7971
Kirk.bailey@seattle.gov