HOMELAND SECURITY:

CYBER-SECURITY AT THE LOCAL LEVEL

Kirk Bailey, CISSP, CISM
CISO, UW

Ernie Hayden, CISSP
CISO, Port of Seattle
U.S. CRITICAL INFRASTRUCTURE

SOME RELATED FACTS... FOR CONTEXT

HOW BIG?
300 Inland // Costal Ports
87,000 Localities // Jurisdictions
80,000 Dams
2,800 Electrical Power Plants
104 Commercial Nuclear Power Plants
2,000,000 Miles of Pipelines
2,250,000,000 Miles of Telecommunication Cables
1,800 Federal Water Reservoirs
1,600 Municipal Wastewater Facilities
5,000 Public Airports
120,000 Miles of Major Railroads
5,800 Registered Hospitals
66,000 Chemical Plants (Hazardous Materials)
460 Skyscrapers
26,600 FDIC Insured Financial Institutions
1,912,000 Farms
87,000 Food Processing Plants
SEATTLE'S SLICE OF THE PIE...
160,000 JOBS GENERATED IN THE REGION

$5.5 BILLION PAYROLL

$12 BILLION REVENUE

$660 MILLION STATE & LOCAL TAX GENERATION

DIVERSE INFRASTRUCTURE AND SERVICES

AIRPORT, SEAPORT, FISHING TERMINAL, PARKS & RECREATION FACILITIES

POLICE, FIRE & EMS SERVICES
- 196 ACRES
- ON-DOCK RAIL
- 5 BERTHS
- 8 CONTAINER CRANES

TERMINAL 18

COSCO
China Shipping
Columbus Line
Hapag Lloyd
K-Line
Lykes Line
Maruba Line
Matson Navigation
NYK
Norasia/CSAV
OOCL
P & O Nedlloyd Ltd.
TMM
Yang Ming Line
ZIM
Value of Trade
$23.8 Billion
Imports: $18.5B
Exports: $5.3B
<table>
<thead>
<tr>
<th>Year</th>
<th>Vessels</th>
<th>Pax</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>6</td>
<td>7,000</td>
</tr>
<tr>
<td>2001</td>
<td>58</td>
<td>170,000</td>
</tr>
<tr>
<td>2003</td>
<td>100</td>
<td>400,000</td>
</tr>
<tr>
<td>2004</td>
<td>150</td>
<td>560,000</td>
</tr>
<tr>
<td>2005</td>
<td>170</td>
<td>650,000</td>
</tr>
</tbody>
</table>

**Cruise Ships**
• **POWER**
  - SEATTLE CITY LIGHT // PUGET SOUND ENERGY

• **SEWER**
  - CITY OF SEATTLE // KING COUNTY

• **WATER**
  - SEATTLE PUBLIC UTILITIES // LOCAL WATER DISTRICTS

• **TELECOMMUNICATIONS**
  - QWEST // AT&T (Cell) // NEXTEL (Cell) // VERIZON
  - WESTON BUILDING // FISHER PLAZA
  - CITY OF SEATTLE FIBER AND STREET RIGHT OF WAYS

• **800 MHz // 911**

• **PUBLIC SAFETY**
  - POLICE // FIRE // EMERGENCY OPERATIONS (EMS)
• TRANSPORTATION
  – HIGHWAYS: I-5 // I-90 // I-405 // 520
  – VIADUCT // US-99
  – CITY SURFACE STREETS and BRIDGES
  – CITY TRAFFIC CONTROL SYSTEMS

• PIPELINES
  – WATER: SEATTLE PUBLIC UTILITIES & LOCAL DISTs
  – AVIATION FUEL TRANSPORT: OLYMPIC PIPELINE
  – NATURAL GAS: PUGET SOUND ENERGY

• RAILROADS
  – BNSF // UNION PACIFIC

• BANKING // FINANCE
  – FED. RESERVE // B of A // WAMU // BANK OF CAL.

• INFORMATION SYSTEMS
THE BIG COMBINED CYBER PICTURE

- 14,000+ DESKTOPS and LAPTOPS
- 2,500+ SERVERS
- 1500+ NETWORK PERIPHERALS (printers, fax)
- 4,500+ RADIOs (all types)
- 3,000? PDAs // TREOS // BLACKBERRIES
- 18,000+ TELEPHONES (desk and cell)
- 5,000? MILES of FIBER and CABLE
- 100+ UNIQUE or SPECIALIZED INFO. SYSTEMS
PROTECTING CRITICAL SERVICES LIKE PUBLIC SAFETY OR POWER AND WATER SUPPLIES IS VERY DIFFERENT THAN SIMPLY PROTECTING COMPUTERS, NETWORKS, AND DATA FROM HARM.

IF YOU THINK BEING A SUPER GEEK OR A NETWORK SPECIALIST IS ENOUGH... YOU WILL FAIL AND AND PEOPLE WILL BE HARMED.
Security Profession Expertise Levels

Strategic Security
- Terrorism
- Regional Interests
- Nation State Interests
- Intelligence
- Active Defense Continuum
- Professional Alliances
- Politics
- Strategies and Tactics

Information Security
- Risk Management
- Intellectual Property
- Business / Financial Integrity
- Regulatory Compliance
- Organized Cyber-Crime
- Industrial Espionage
- Privacy
- Forensics & Investigations

Technology Security
- Firewalls
- Intrusion Detection
- Network Security
- Viruses, Worms, Crimeware
- System Hardening
- Encryption
- Engineering

Business Problems
- Intellectual Property
- Business / Financial Integrity
- Regulatory Compliance
- Organized Cyber-Crime
- Industrial Espionage
- Privacy
- Forensics & Investigations

Critical Security Problems
- Terrorism
- Regional Interests
- Nation State Interests
- Intelligence
- Active Defense Continuum
- Professional Alliances
- Politics
- Strategies and Tactics

Chart Based on Forrester, April 2005
THE NEED FOR INTELLIGENCE

SECURITY PROFFESIONALS NEED TO KNOW THE **WHO**, **WHAT**, **WHERE** AND **WHY** BEHIND ALL THE FRUSTRATING, MISERABLE AND HARMFUL STUFF TO FIGURE OUT **HOW** TO DEAL WITH IT ALL.

“In the world of networked computers every sociopath is your neighbor.”

- Dan Geer, Chief Scientist, Verdasys
A NETWORK OF TRUST

YOU HAVE TO REMAIN HUMBLE AND KNOW YOUR LIMITS
... AND KNOW EVERYONE WHO CAN HELP YOU.
Civil Liability Arising from Cybercrimes

Tort Liability Requires:

- A definable duty of care owed by one class of persons to another.
- A breach of that duty of care by a person owing a duty of care.
- Harm caused by the breach to a person owed the duty of care.
- Causation (i.e., Liability) depends on foreseeability of harm.

Risk Management Methodology

Value of a safeguard is different than the cost. Value is estimated as a factor of the Probability of a loss multiplied by the Mitigation value of safeguard.

\[ V_{\text{(value of safeguard)}} = P_{\text{(probability)}} \times C_{\text{(cost)}} - M_{\text{(mitigation by safeguard)}} \]

Also the Value of a safeguard must be greater than (or equal to) the Costs of the safeguard.

\[ V_{\text{(value of safeguard)}} \geq C_{\text{s(cost of safeguard)}} \]
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.”
Cyber-based Terrorist Threats: Analysis for The City of Seattle, and The State of Washington

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

Confidential

(Disclosure Protection provided under WA State RCWs)

Prepared by: Kirk C. Bailey, CISSP, CISM
CISO, City of Seattle
PC Zombies and botnets

...and other stuff
RAPIDLY GROWING THREAT SPECTRUM

CRIMINAL ELEMENTS ARE ACTIVELY FINANCING AND WORKING TO CONTROL MALWARE DEVELOPMENT AND DELIVERY SYSTEMS.

SERIOUS CRIMINALS ARE NOW SEEKING CONTROL OF BOTNETS AND IMPROVING HOW THEY COVER THEIR TRACKS AND FOIL INVESTIGATIONS.

THE NEW CRIMINAL ACTIVITIES AND INVESTMENTS ARE PRODUCING “CRIMEWARE” WITH BETTER TARGETING, PAYLOAD AND DELIVERY SYSTEMS.

IT ALL MEANS THAT “ZERO DAY” EVENTS ARE MORE LIKELY WITH EVEN WORSE IMPLICATIONS THAN IMAGINED BEFORE.
A NETWORK OF TRUST

A VIEW OF A SMALL PORTION OF ORGANIZED CYBER-CRIME AND GEOGRAPHY OF EVOLVING “CRIMEWARE”

CODERS FOR HIRE

SOME CODERS ARE FLAMBOYANT IN THE ONLINE UNDERGROUND AND THEIR ONLINE COMMENTS ARE MONITORED.

CYBER-CRIME GANGS

PHISHING GROUPS (PGs) PROFILED AND TRACkED BY ANTI-PHISHING WORK GROUP

A NETWORK OF TRUST
WHAT ARE THEY DOING?

TERRORISM?

ILLEGAL DRUGS
- HEROIN
- COCAINE
- MARIJUANA
- METH
- PRESCRIPTION DRUGS

HUMAN TRAFFICKING

SLAVERY

PROSTITUTION

CHILD PORN

Porn

TERRORISM?

ILLEGAL WEAPONS

ILLEGAL DRUGS

MONEY LAUNDERING & MOVEMENT

MARIJUANA

COCaine

HEROIN

ILLEGAL DRUGS

ELECTRONIC THEFT & FRAUD

"CRIMEWARE"

CREDIT FRAUD

FEE SCAMS

ID THEFT

STOCK FRAUD & SHARE MANIPULATION

SOFTWARE PIRACY

ELECTRONIC EXTORTION

INFORMATION THEFT & SALES

INDUSTRIAL ESPIONAGE

ILLEGAL WEAPONS

MONEY LAUNDERING & MOVEMENT

WHAT ARE THEY DOING?

= TRADITIONAL INTERNATIONAL CRIME
International Exercises – US / Canada

• TopOff2
• Livewire
• BlueCascades II
• ALKI

Vulnerability Exercises

• City of Seattle’s “ALKI”

Tabletop Exercises Underscore Criticality of Cyber-Issues

International Exercises – US / Canada
THINGS TO THINK ABOUT IF YOU WANT TO BE A CYBER-SECURITY PROFESSIONAL

The Hot Seat
Impact on Peoples’ Lives
Background Checks // Your Privacy
The Adversary
Questions?