# Threat Management

## Towards a quantitative analysis

Seth Bromberger
Principal, NCI Security LLC
seth@ncisecurity.com

"

In another testament to the fact that some of the

**brightest security research**

is coming out of the nation's critical infrastructure operations, researchers at [PG&E] have... fine-tuned a homegrown methodology for doing quantitative threat analysis.

"

*Information Security* Magazine, Editor's Corner, March 2008

The Threat / Vulnerability Management developed and fully implemented within PG&E provides one of the most

**comprehensive risk management**

modeling and monitoring tools that this team has seen to date.

Security Horizons IA-CMM Final Report, on behalf of the US National Security Agency, October 2007

$$R = T \quad V \quad C^{*}$$

$^{*}$ or $I$

# T = 1 ?!

Irresponsible.

# Goals

Quantitative Approach

Consistent Methodology

IA-CMM PA04 / OpSec Step 2

Cheap

# Threats, Defined

Means

Motive

Opportunity

# Threat Matrix Development

# Define Threats

Insiders

Domestic Activists

WFNS

Define Threats

## Define Capabilities and Levels

Size

Funding

Knowledge

Size

Funding

Knowledge

| Level | Description |
|---|---|
| 0 | no people |
| 1 | individual, no collusion |
| 2 | 2 - 10 people |
| 3 | 11 - 100 people |
| 4 | 101 - 1000 people |
| 5 | 1000+ people |

Define Threats

Define Capabilities and Levels

Apply Levels to Threats

|  |  | Capability |  |  |
|---|---|---|---|---|
|  |  | Size | Funding | Knowledge |
| Threat Agent | Insiders | 1 | 1 | 5 |
|  | Domestic Activists | 3 | 3 | 2 |
|  | WFNS | 5 | 5 | 4 |

Define Threats

Define Capability Levels

Apply Levels to Threats

Periodic Updates

How are

**THREATS**

&

**VULNERABILITIES**

related?

# The Vulnerability Connection

| | Size | Funding | Knowledge |
|---|---|---|---|
| Insiders | 1 | 1 | 5 |
| Domestic Activists | 3 | 3 | 2 |
| WFNS | 5 | 5 | 4 |

# Requirements

| Vulnerability X | Size | Funding | Knowledge |
|---|---|---|---|
| Vector 1 | 1 | 3 | 5 |
| Vector 2 | 5 | 1 | 3 |

| Vulnerability X | Size | Funding | Knowledge |
|---|---|---|---|
| Vector 1 | 1 | 3 | 5 |
| Vector 2 | 5 | 1 | 3 |

|  | Size | Funding | Knowledge |
|---|---|---|---|
| Insiders | 1 | 1 | 5 |
| Domestic Activists | 3 | 3 | 2 |
| WFNS | 5 | 5 | 4 |

| *VECTOR 1* | Size | Funding | Knowledge | Sum |
|---|---|---|---|---|
| Insiders | 0 | -2 | 0 | -2 |
| Domestic Activists | 0 | 0 | -3 | -3 |
| WFNS | 0 | 0 | -1 | -1 |

WFNS (-1)

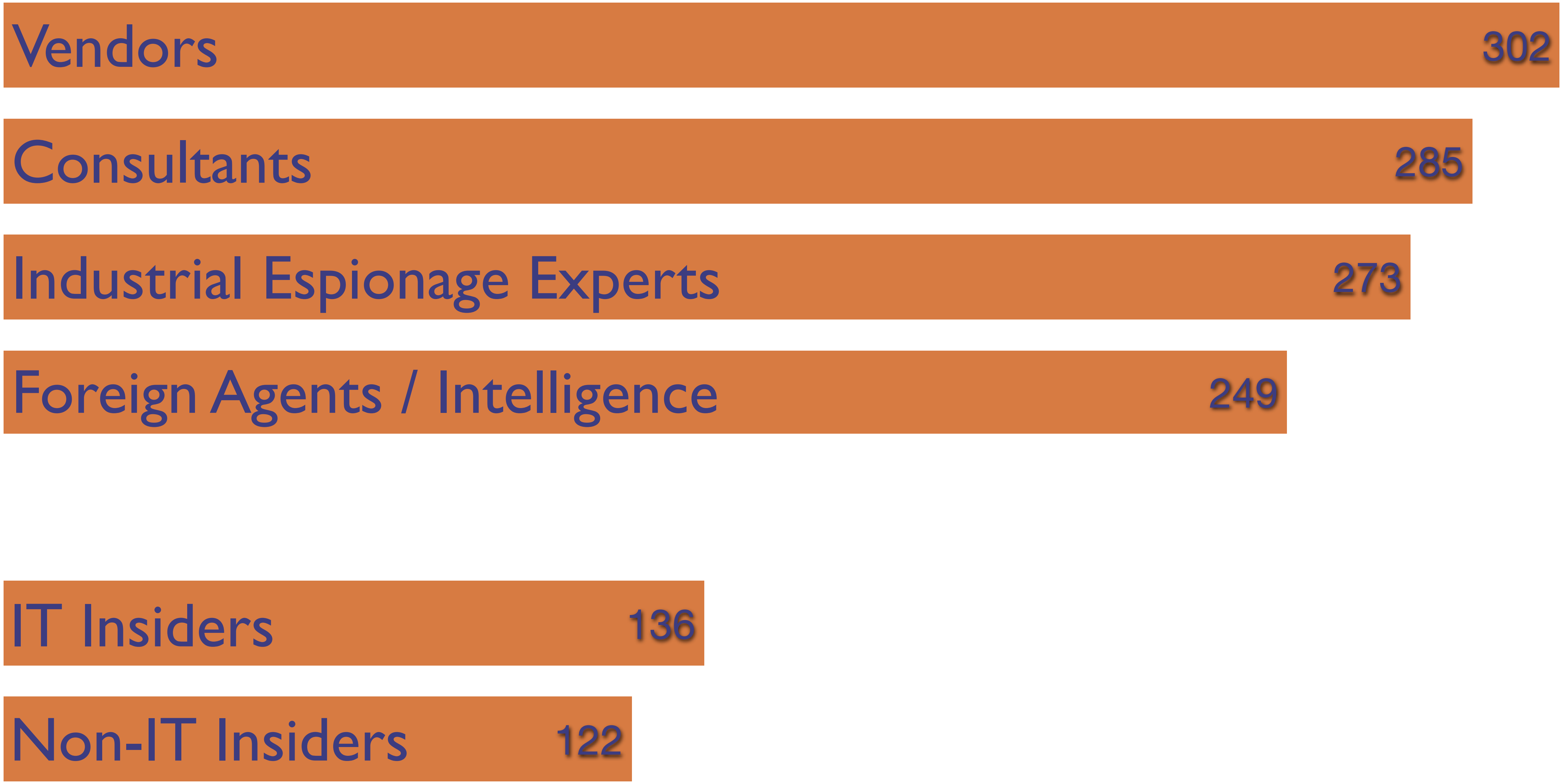
Insiders (-2)

Domestic Activists (-3)

# Strategic Planning

# Top & Selected Threat Agents

first three months, n=487



# Results of Program

AURORA

IA-CMM

Accolades

DHS researchers ... successfully destroyed a generator through an experimental cyber attack. This experiment was code-named "Aurora."

Officials tell me that malicious actors – insiders, terrorists, or nation states – could use the same attack vector against larger generators and other critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure.

http://langevin.house.gov/news/speeches/2007/10/stmtcyber101707.shtml

# *"...insiders, terrorists, or nation states..."*

| | |
|---|---|
| Partners (Vendors, Contractors, Consultants) | -1 |
| Operations Employees | -3 |
| Foreign Agents / Intelligence | -3 |
| Industrial Spies | -3 |
| Other Insiders | -3 |

In a recent 2007 INFOSEC Assessment administered by the National Security Agency (NSA), PG&E received ... the

**second highest rating**

ever given out by the NSA in the INFOSEC Assurance – Capability Maturity Model (IA-CMM) category.

Forrester Total Economic Impact™ Study, February 2008

# شكراً

# Thank you!

http://www.ncisecurity.com

http://www.bromberger.com