Bay Area UASI Homeland Security Strategy Briefing

Alameda, California

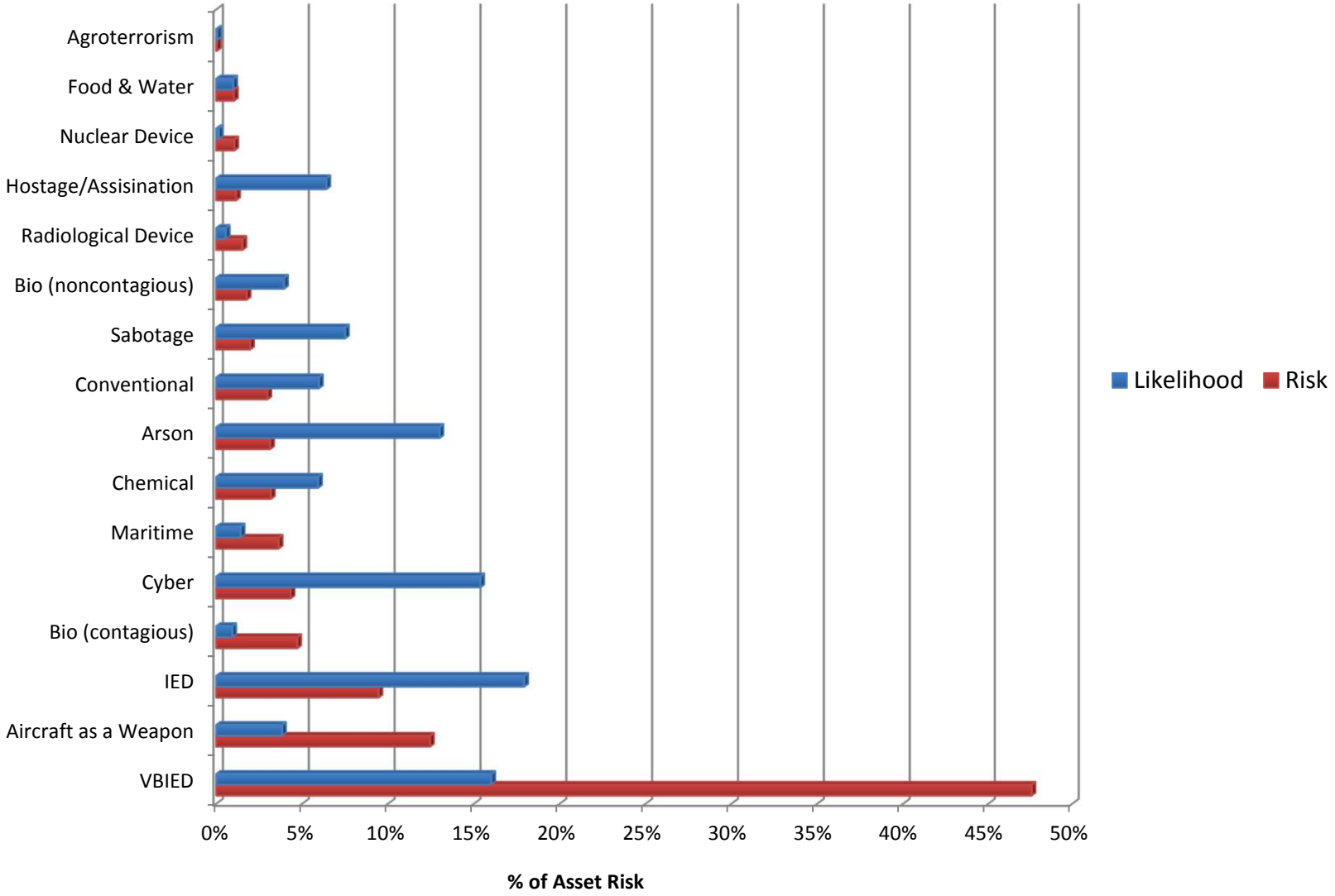
October 10, 2013

FILLER SECURITY STRATEGIES, INC.

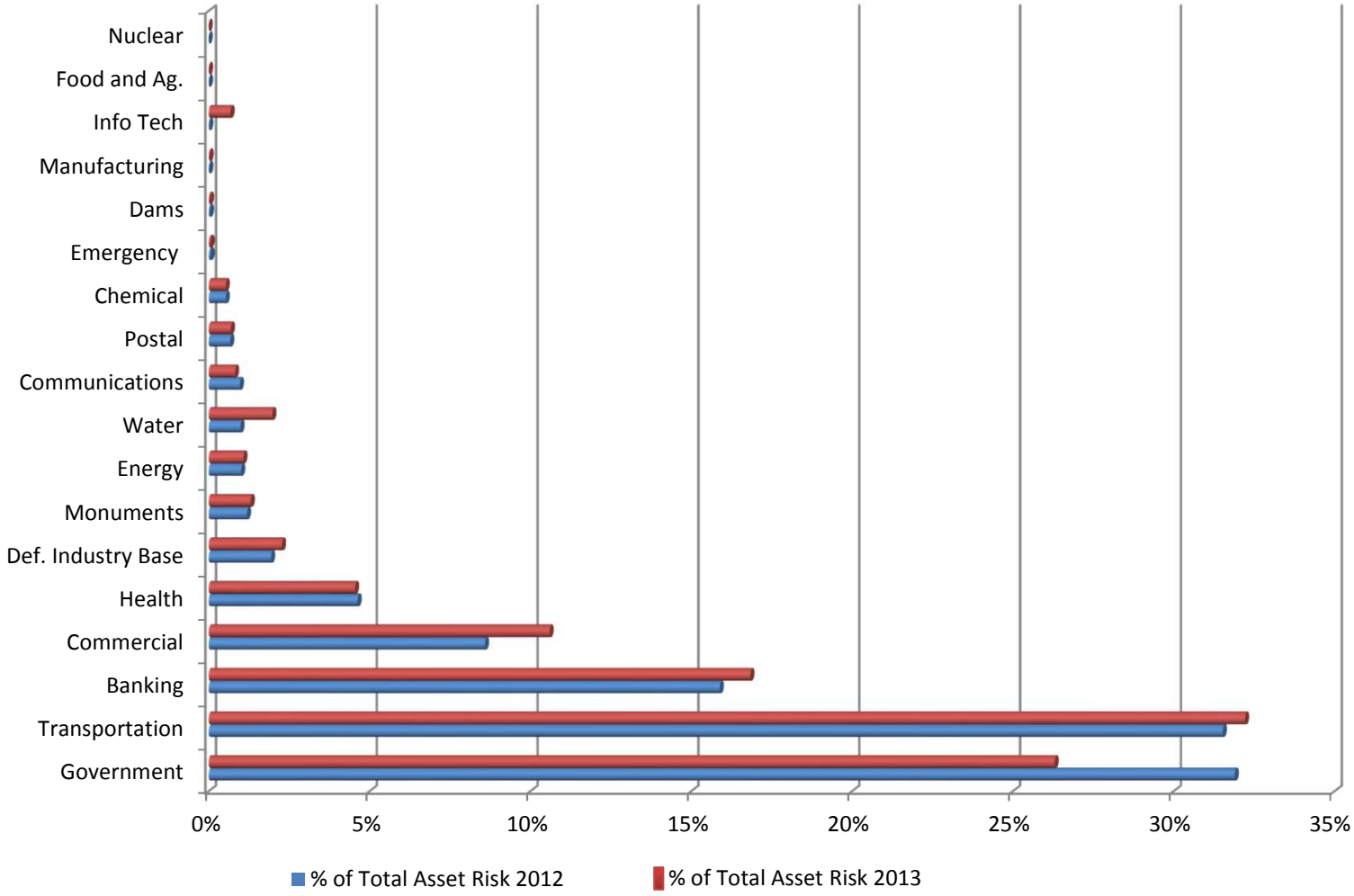
Major Strategy Changes in 2013

- Updated Regional Risk Profile - added 4,500 assets (now approximately 13,000 in the risk analysis center).
- Developed Bay Area Compendium of Core Capabilities with locally tailored preparedness measures and metrics for all 31 Core Capabilities.
  - Conducted OA/Major City level assessments and one regional assessment.
- Developed a new Cyber Security Objective - 2.4.

Terrorism Risk Assessment Findings by Scenario
Risk versus Likelihood



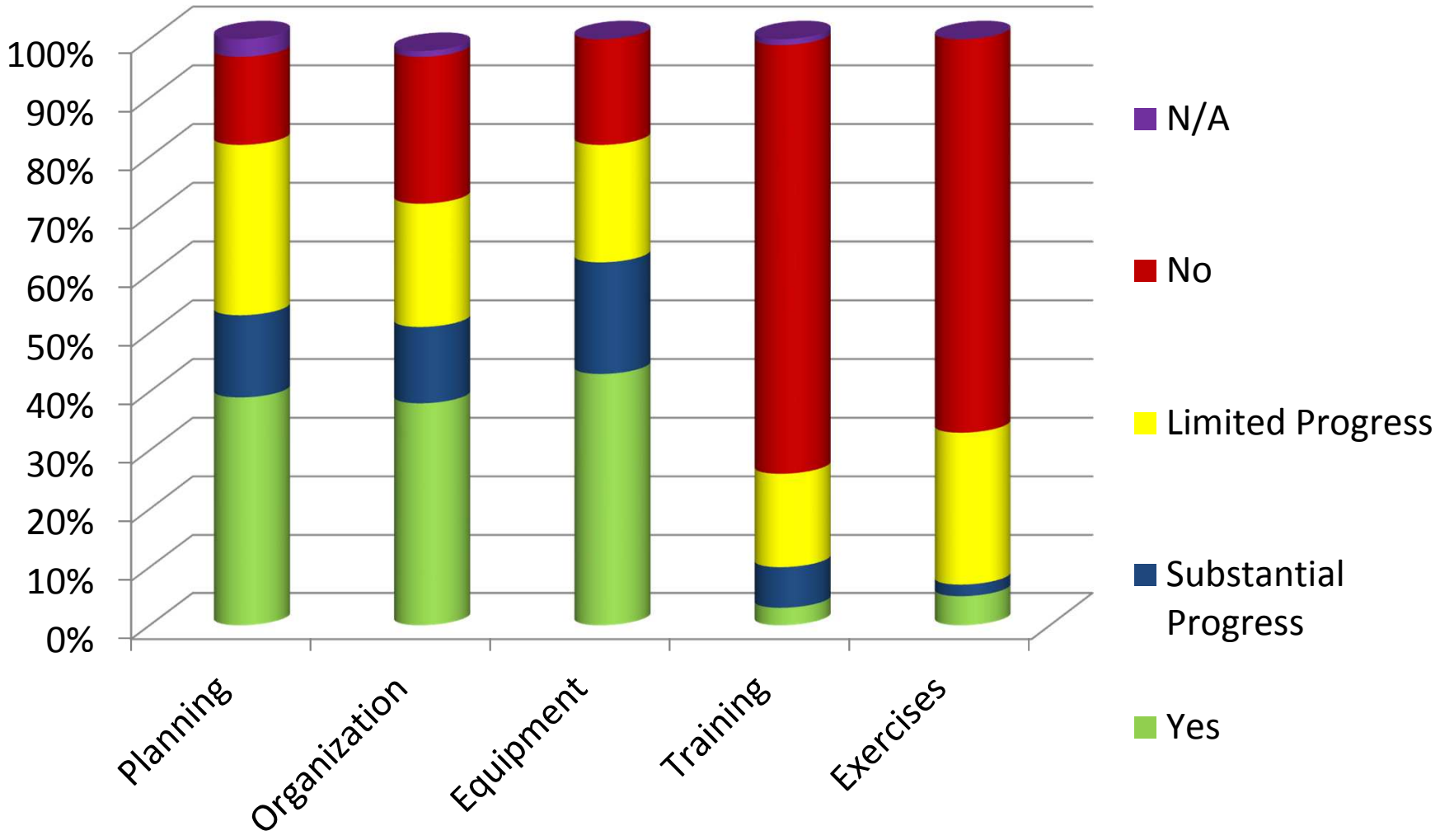
Terrorism Asset Risk by Sector 2012 versus 2013



2013 Risk and Capabilities

Risk and Gap	Core Capability	Risk Relevance	Level of Ability	Gap Analysis
1	Infrastructure Systems	3	25%	Needs Extra Attention
2	Long Term Vulnerability Reduction	6	31%	Needs Attention
3	Physical Protective Measures	7	39%	Needs Attention
4	Public Information and Warning	9	26%	Needs Attention
5	Operational Communications	16	34%	Needs Attention
6	Community Resilience	1	69%	Needs Attention
7	Intelligence and Information Sharing	4	55%	Needs Attention
8	Planning	8	58%	Needs Attention
9	Situational Assessment	12	57%	Needs Attention
10	Screening, Search and Detection	14	68%	Needs Attention
11	Forensics and Attribution	2	79%	Sustain
12	Interdiction and Disruption	5	70%	Sustain
13	Risk and Disaster Resilience Assessment	10	90%	Sustain
14	Risk Management for Protection Programs	11	82%	Sustain
15	Threats and Hazard Identification	13	84%	Sustain
16	Operational Coordination	15	80%	Sustain
17	Access Control and Identity Verification	18	34%	Needs Attention
18	Critical Transportation	21	27%	Needs Attention
19	**Cyber Security**	20	33%	Needs Attention
20	Natural and Cultural Resources	28	30%	Sustain
21	Public Health and Medical	19	67%	Sustain
22	Fatality Management	21	61%	Sustain
23	Mass Search and Rescue	23	69%	Sustain
24	On-Scene Security and Protection	18	85%	Sustain
25	Supply Chain Integrity	26	25%	Sustain
26	Health and Social Services	25	34%	Needs Attention
27	Mass Care	29	42%	Sustain
28	Housing	31	38%	Sustain
29	Environmental Response/Health and Safety	24	82%	Sustain
30	Economic Recovery	27	38%	Sustain
31	Public and Private Services and Resources	30	49%	Sustain

Cyber Security Assessment Findings



Cyber Security Strategic Approach

- Use assessment findings to drive strategic objective and implementation steps.
- Recognize the interrelationship between the physical world and the cyber world.
  - Cyber security and preparedness are not just an IT issue.
  - Often the gateway to the cyber world starts in the physical world.
    - Scams against untrained employees.
    - Unsecure physical locations with portals into critical cyber networks.

2013 Cyber Security Objective

- Getting **organized** – developing cyber focus group and integrate the private sector.
  - NCRIC taking the lead with cyber analytical program

- Develop **plans** – conduct cyber vulnerability assessments on certain networks, and develop basic cyber protocols followed by incident response and continuity plans.

- Conduct **training**. Training will include basic awareness training for all employees up to specialized training for IT professionals and law enforcement.