When the Ecosystem Works: Best Principles for ISAOs

Bonnie Moss
Executive Director

SMBiSAO

SURPRISING FACT

What is an Ecosystem?

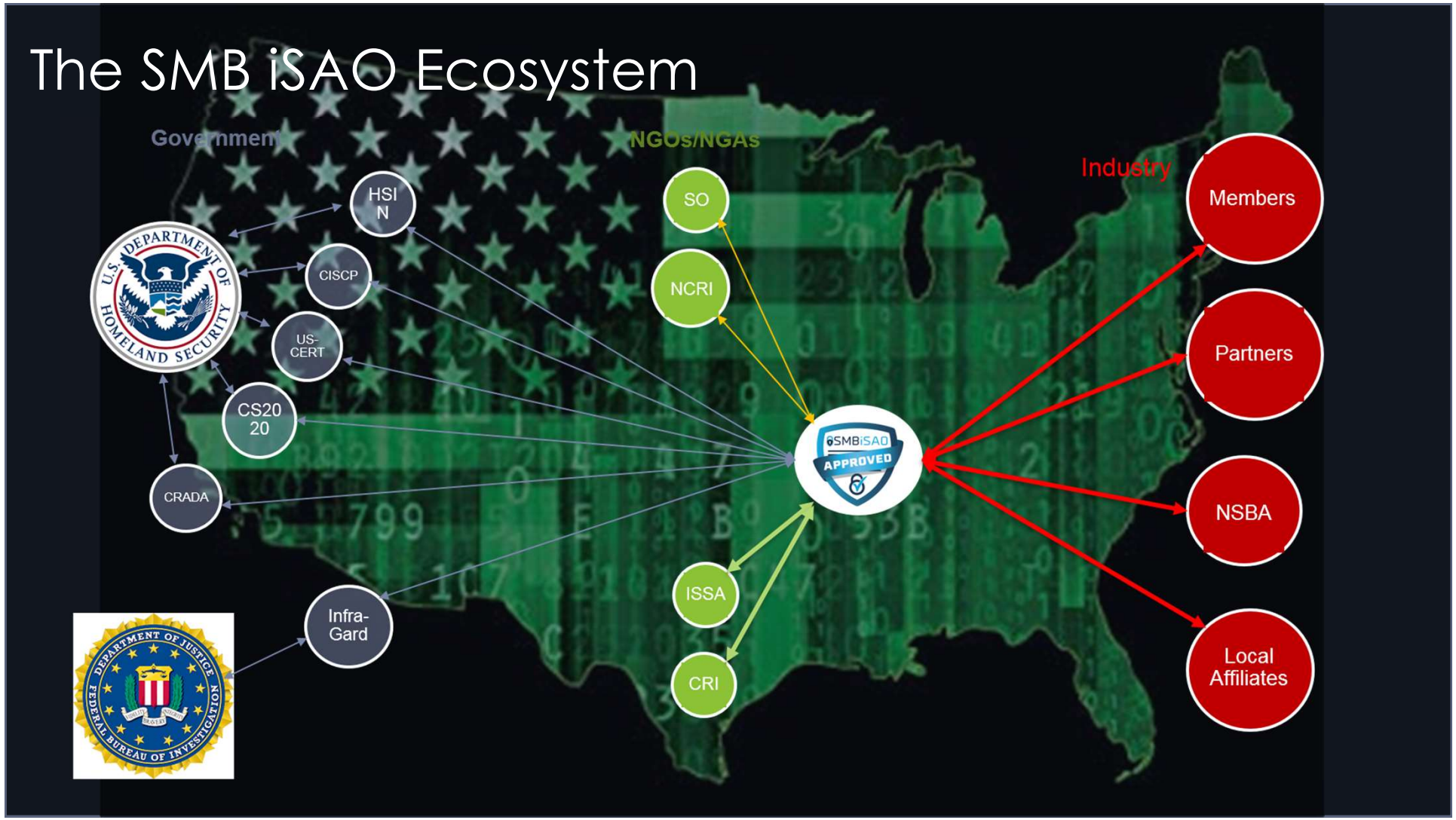
- a complex network or interconnected system
- a biological community of interacting organisms and their physical environment

SMBiSAO

Who plays a role?

SMBiSAO

The SMB iSAO Ecosystem



What makes it work?

- Biological systems work because members don't deviate from genetically programmed roles.
- The Info Sharing Ecosystem involves people. People have choices.

SMBiSAO

When it works

GOOD: Information Sharing

BETTER: Collect, share, analyze and create data into actionable intelligence

BEST: The whole is greater than the sum of its parts

SMBiSAO

What makes it work?

What is looks like when it does *not* work:

- Does not produce actionable CTI;
- Submitting redacted reports with only an IP address
- No Push / No Pull
- Inefficient uses of classifications

SMBiSAO

Participants in the ecosystem?

- Are leaders leading?
- Are members sharing?
- What is beyond minimum requirements of participation?
- How can we exceed standards?

SMBiSAO

This is NOT an ecosystem:

Collecting data does not qualify you as an information sharing organization; it qualifies you as a collection agency.

SMBiSAO


ISAO
Standards Organization

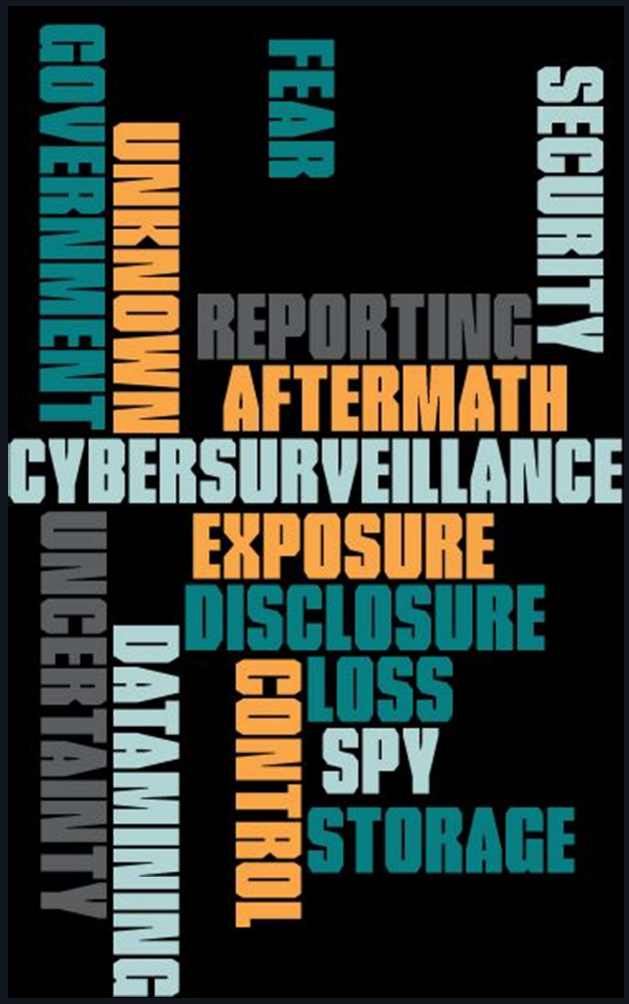
Looks Great On Paper!

…but obstacles loom…

SMBiSAO

Obstacle: Trust

"Our civil liberties and right to privacy should not be the price we pay for security."



Sharing Obstacle: The Hacked Mindset

The information sharing ecosystem suffers from a common tragedy: everyone wants to receive CTI, but few are prepared to share, **especially** after a hack.

SMBiSAO

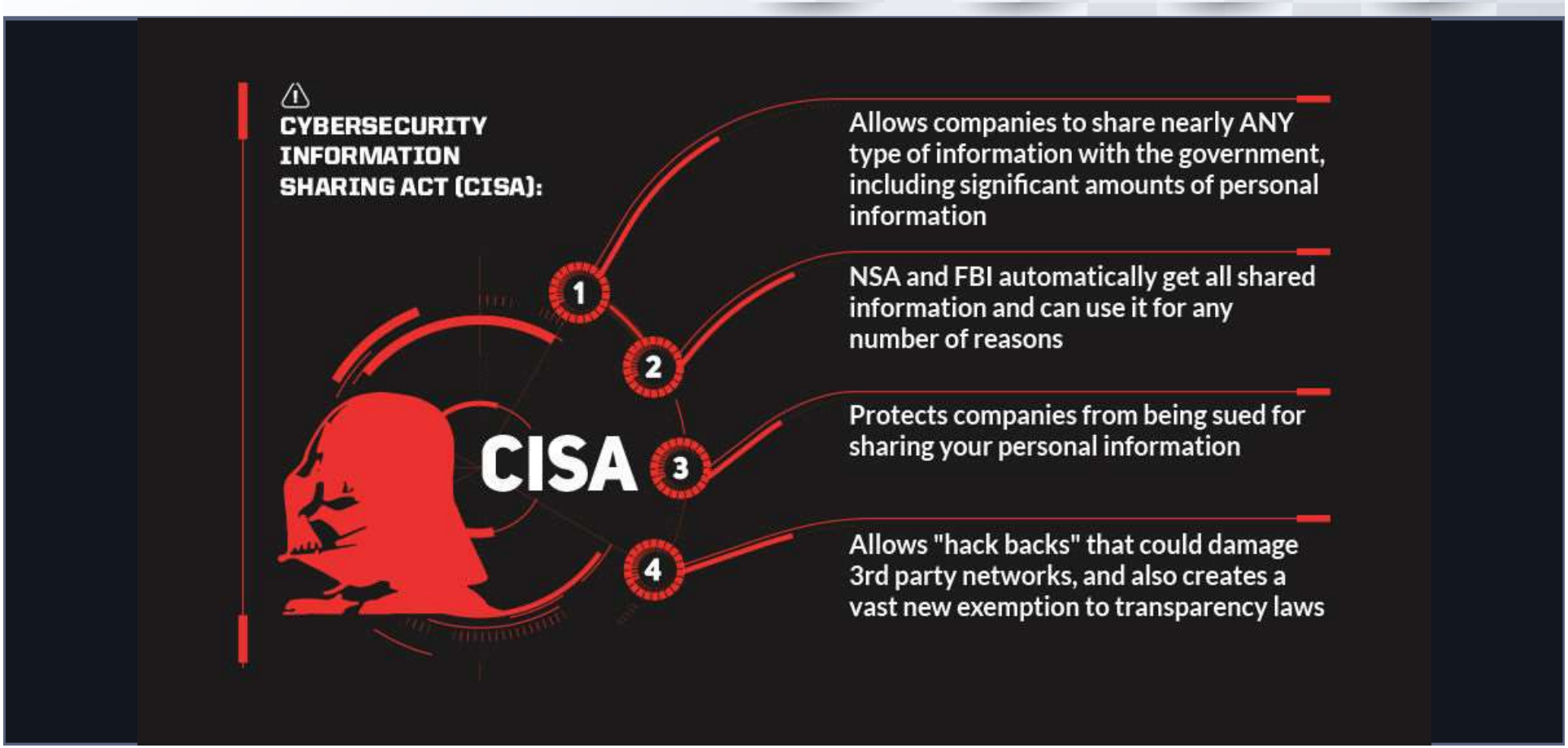
Obstacle: The Corporate Mindset

Concerns:

- PR damage
- Losing customers
- Compliance regulations
- Fear of surveillance
- Losing stakeholder confidence
- Cost
- Incurring legal liabilities

SMBiSAO

A Surveillance Bill In Disguise!



The Underlying Fear

Fear of reporting a breach is still greater than the fear of the breach itself.

SMBiSAO

Obstacle: Logistics

- DHS AIS program integration
- Delays in distribution of attack indicators
- Private sector executives with clearance have access to classified data but can't share.

SMBiSAO

Obstacle: Technical

- 500 shared instances can equal tens of thousands of threat indicators.
- "Scrubbed" or anonymized information = more difficult to use.
- Potential for human error.
- Anyone can start an ISAO.

SMBiSAO

Meaningful Reporting

- Incident Reporting Form for:
  - attempts to gain unauthorized access to a system or its data,
  - unwanted disruption or denial of service, or
  - abuse or misuse of a system or data in violation of policy.
- Share indicators and defensive measures
- Report software vulnerabilities or Industrial Control System vulnerabilities
- Report phishing
- Report malware

SMBiSAO

Solution: Keep it Simple

- Each ISAO and ISAC should operate in a trust environment with each other.
- Analysts need to be able to jump on the phone with one another and get more context than just a malicious IP.
  - Typical Sample Report : 192.168.1.1
  - Better Sample Report: Experienced a SYN Flood attack on port 45 from 192.168.1.1 on July 4th, 1776.

SMBiSAO

The Human Factor

- ❑ You can't build and run an ISAO on technology.
- ❑ N-ISAC snapshot
- ❑ Cybersecurity is a team sport.

.

People make it work, not technology.

SMBiSAO

Solution: Keep it Simple

- Make it easy for people to do.
- Trust is critical.
- Testimonials and success story encourage sharing.
- Members of ISAOs and ISACs need to discerningly ingest and apply the intel received.
- The best intel is what you generate yourself. Having the ability to analyze intel prior to putting it into active monitoring mode is crucial.

SMBiSAO

“Wars may be fought with weapons, but they are won by man.” --Patton

Questions? Find me at:

bonnie.moss@smbisao.com

SMBiSAO