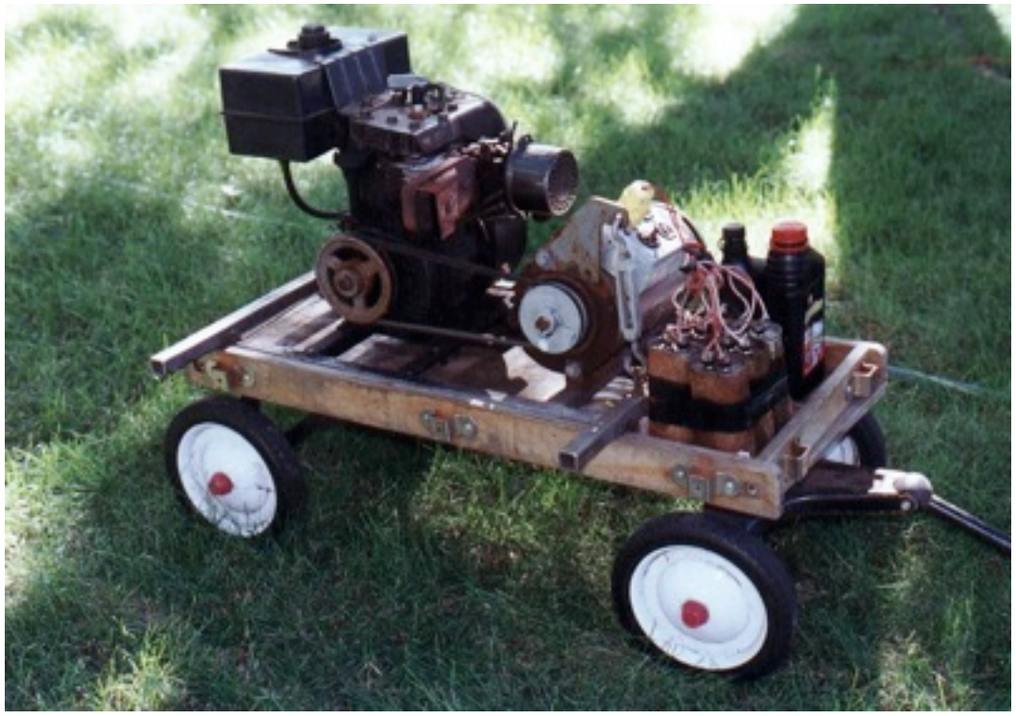


Incident Response:

Small & Medium Sized Utility Considerations

Agenda

- Introductions
- The Electric Grid: Not a Primer
- The Problem Space
- Shifting Scope
- Solutions?

Introductions

- Jack Whitsitt | jack@energysec.org | http://twitter.com/sintixerr
  - Broad Background
    - Lived in a little hacker compound as a kid
    - Started with Open Source development (Rubicon03)
    - MSSP:IDS, Data Viz, Anomaly Detection Designer
    - Enterprise Security Architecture
    - ICS-CERT (INL)
    - Fed with Nationally-scoped cyber responsibilities
  - Now: Framing, Lensing, Slicing, Dicing
    - Non-profit Community Builder & Facilitator
    - Focus on Electric Sector

Introductions

- Gal Shpantzer
- 12 years in infosec in private sector (some .edu)
- Security Outliers Project, focusing on culture as security overlay
- Recently: EnergySec.org, worked on ES-C2M2 in 2012 w/ DOE/DHS
- Now: Reviving PACS-WG

The Grid

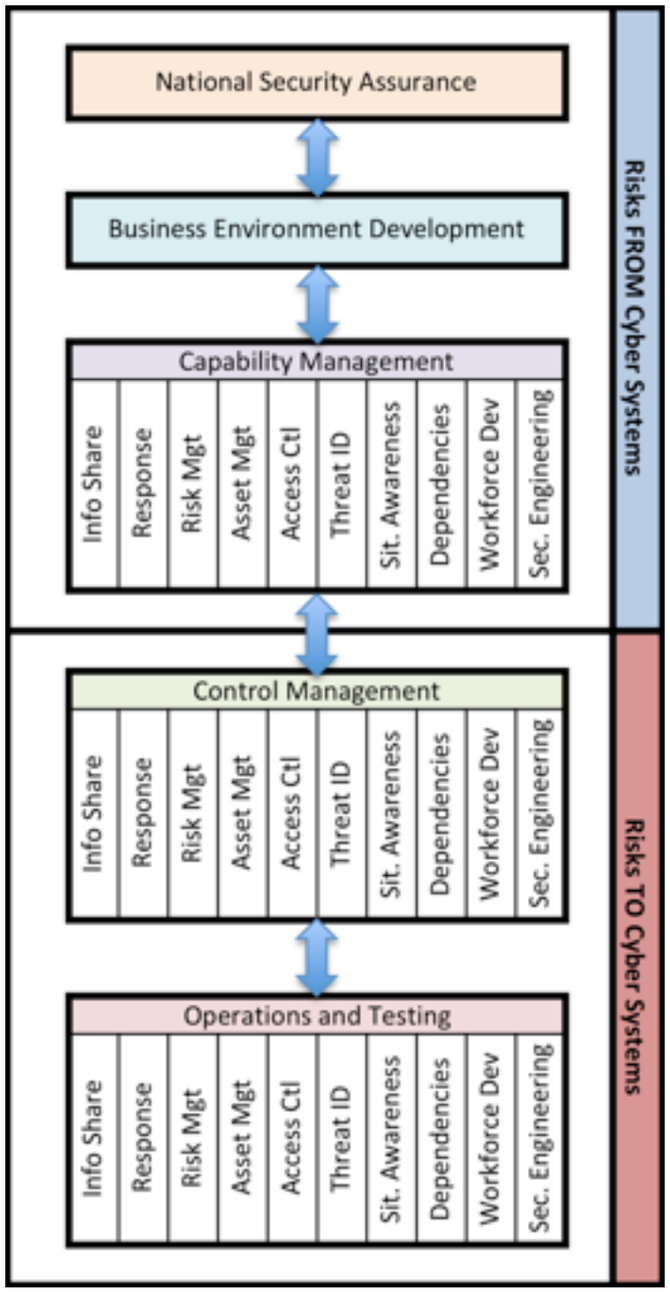
- This isn't a primer!
  - You'll see why later (we hope)

- ...but several obvious points are worth noting...
  - Starting with..it's important!
    - A lot of issues will work out naturally over time
    - Can we wait to do something productive?
  - ...followed by...It's a grid!
    - Electrical sense...
    - ...but also support model – very porous "process" perimeter
  - ...which means...
    - Big, middle, small utilities are all important

Utility Space

- Technology
  - Expensive Equipment
  - Lifetimes in Decades
- Reliability
  - B-SidesDC Example
- Culture
  - Slow to change, slow to accept new perspectives
- Finances and (Business) Regulation
  - Complicated set of restrictions on rates and spending
- Size
  - One kind of problem: Many utilities regulated by NERC CIP
  - Today's kind of problem: Many smaller utilities are not
    - IT Staff? Maybe. Probably. Security? Heh.
    - But. They're. Still. Connected. To. The. Grid.

In a normal world...



...but for small utilities?

Scope Fix Needed (1/3)

- Many “security” best practices are not practical
  - What do I mean by not practical? SANS Example
  - There are efforts to change this, but they’re long-term
    - Executive Order, NIPP, etc. (NERC CIP Another Story)
- No short term solutions makes incident response hard
- How can we start solving?
  - **Without fixing those long term hard problems**
- Framing and lensing to the rescue?...
  - Risks To vs Risks From!

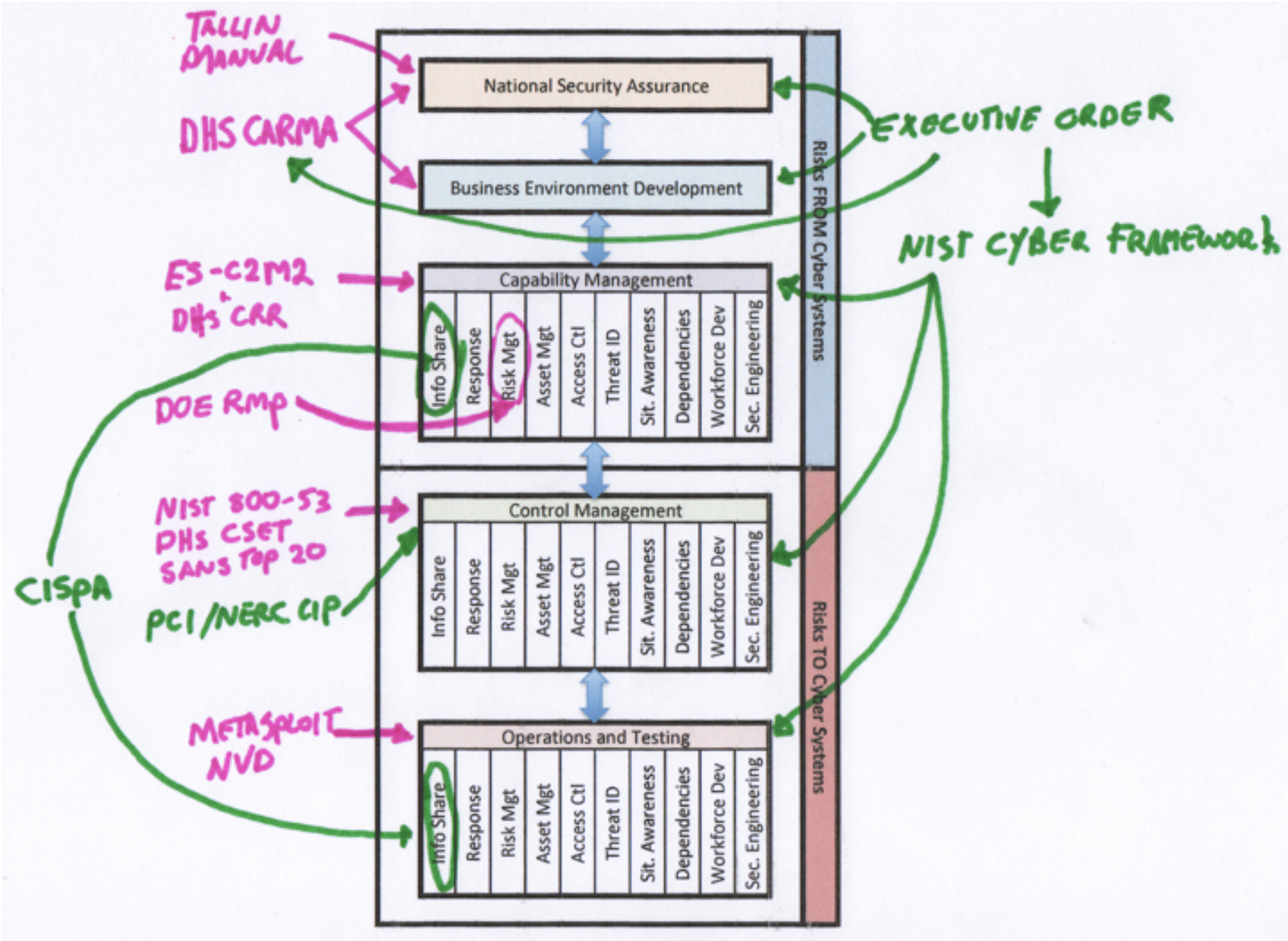
Example Difficulties: SANS 20

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

Scope Fix Needed (2/3)

- Many "security" best practices are not practical
  - What do I mean by not practical? SANS Example
  - There are efforts to change this, but they're long-term
    - Executive Order, NIPP, etc. (NERC CIP Another Story)
- No short term solutions makes incident response hard
- How can we start solving?
  - **Without fixing those long term hard problems**
- Framing and lensing to the rescue?...
  - Risks To vs Risks From!

Making the World Better



Scope Fix Needed (3/3)

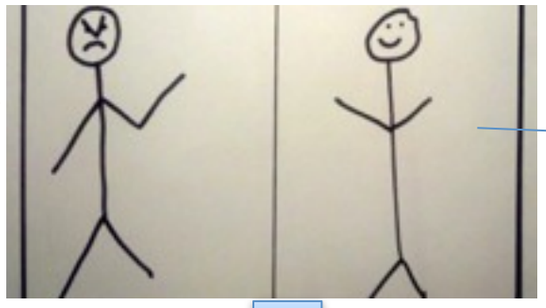
- Many "security" best practices are not practical
  - What do I mean by not practical? SANS Example
  - There are efforts to change this, but they're long-term
    - Executive Order, NIPP, etc. (NERC CIP Another Story)
- No short term solutions makes incident response hard
- How can we start solving?
  - **Without fixing those long term hard problems**
- Framing and lensing to the rescue?...
  - Risks To vs Risks From!

“Security” has natural parenthetical Scopes

Boss Bob

I want to steal hazardous materials!

EVIL GOOD!

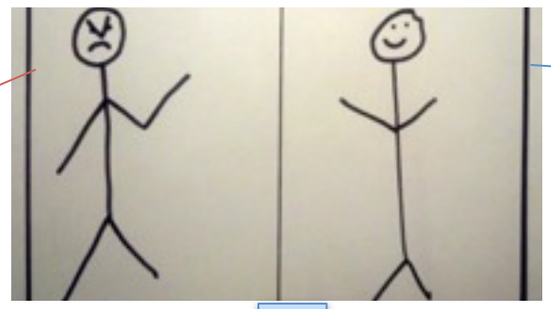


CEO Jim

I want to keep making $123 a day!

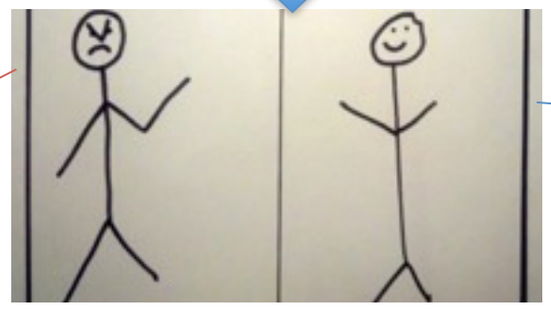
Cyber Planning Bob

Ok, we’ll attack Traffic Light Controls and make trucks stop!



IT Architect Jim

Let’s make sure IT enables $123/day



Hacker Bob

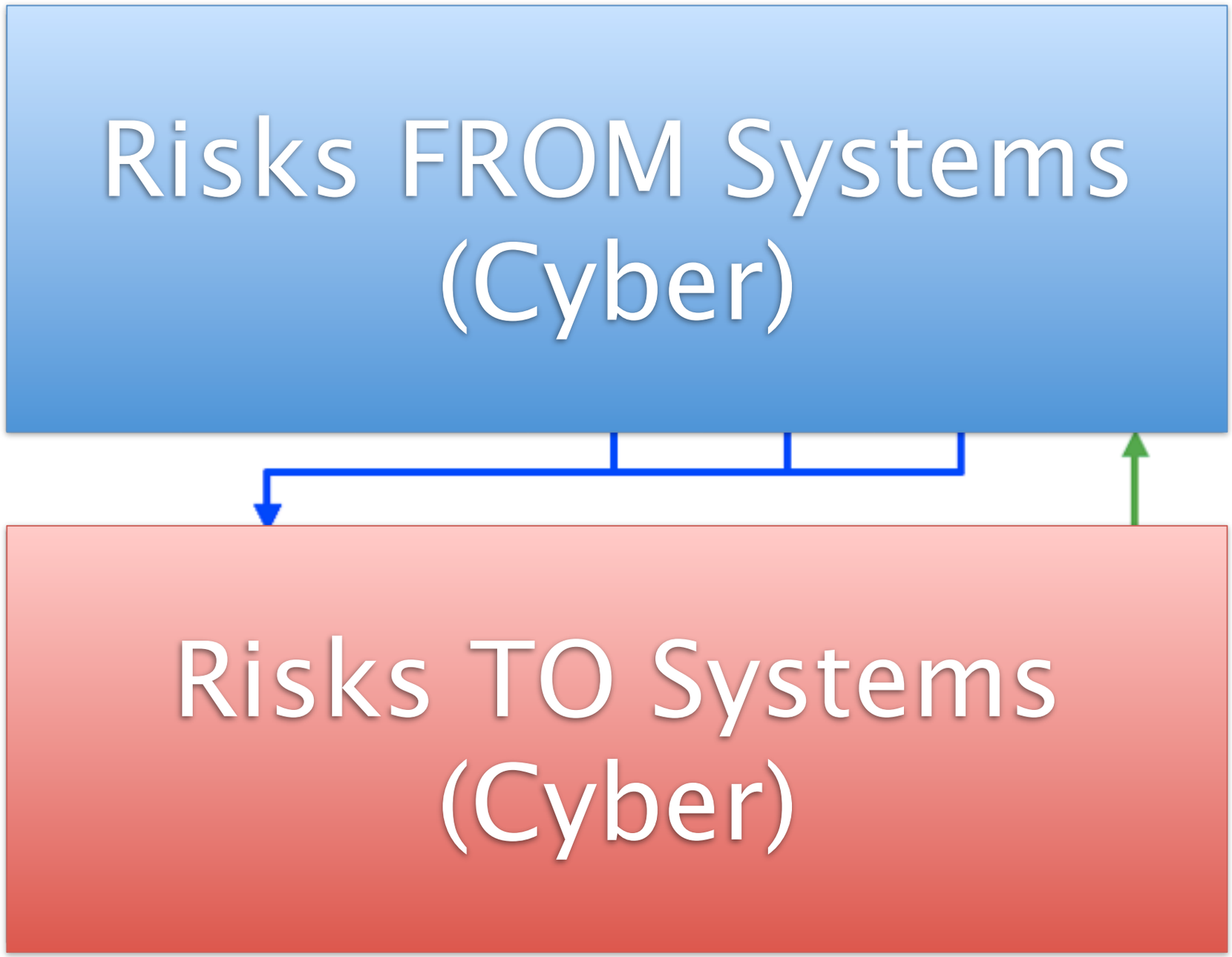
Metasploit to the rescue!

Security Jim

IDS to the Rescue!

“Tech

Articulating Hand-offs is Helpful



Better Framing

- Small / Medium Sized Utilities already equipped to manage some things
  - Risks “From” tend to be business focused
  - Risks “To”, technology centric
  - Utilities can manage existing business more securely?
- Let’s define those boundaries and create hand-offs
  - From “Managed Business” controls
  - To external, tactically applied (contracted?) support
  - And the Cloud!
- We’ve started working on this
  - Controls Which Can Be Executed Without Substantial IT Staff
  - Hand-offs for the rest
  - Incident Management that assumes these hand-offs

Example: Security-less Controls

Manage	Environment	
1. Configurations	Device, Software, Data, Infrastructure, Contracts, Applications	**Risks From**
2. Culture	Awareness, Ownership, Training (this order!)	
3. Access	Monitoring/Control, Admin/Regular	
4. Incidents	Preparation, Identification, Assessment, Reaction, Follow-up	
5. Risk	Business Justifications, Consequence/Dependency Trees	
Outsource	Secure Configs, Vuln Mgt, Application Dev/Hosting, Infrastructure, Ports/Protocols: Cloud or “As Needed”	**Risks To**

Example: Incident Management

- Preparation
  - "Everyone is on the Team", Training and Practice, Contracts
- Identification
  - Can Be Uncomplicated
  - Just need better/more instrumentation (See "What Next!")
  - Internal Knowledge Exists, helps
    - IDS-less SOC Example
    - Back-up Operator Example (FermiLab)
- Assessment, Reaction
  - Call-out
- Follow-up

What Next?

- Packaged Solutions (Products)
  - Hardened Distributions for browser-based operations?

- Community Services (Capabilities!)
  - Baseline Cloud Based Monitoring
  - AntiMalware on endpoints
  - FW Management
  - Information Sharing (not XML-based machine-to-machine)

- Back to graphic of national to tactical. What can be 'communitized' and/or Packaged.