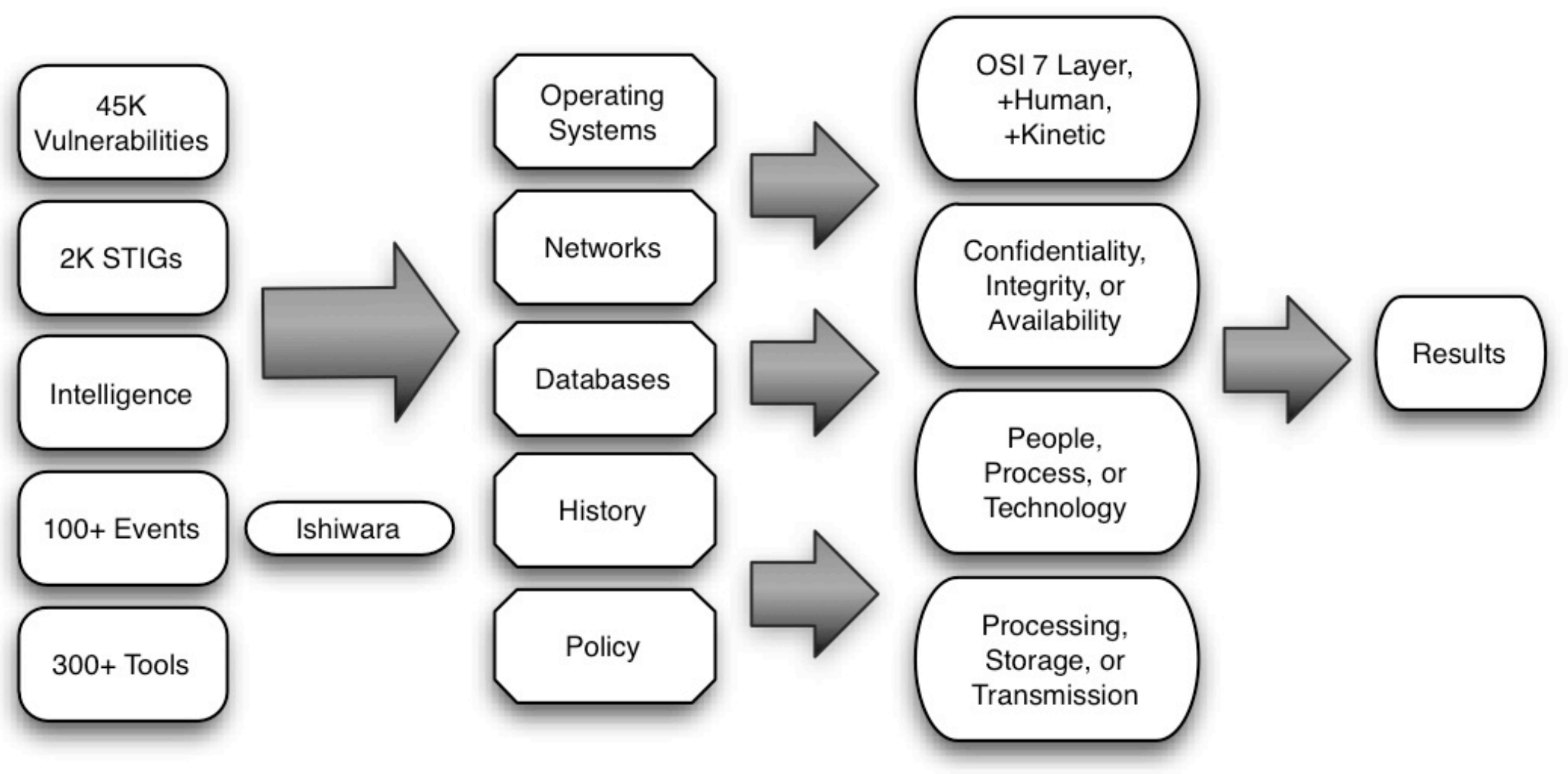
CERIAS
The Center for Education and Research in Information Assurance and Security

PURDUE
UNIVERSITY

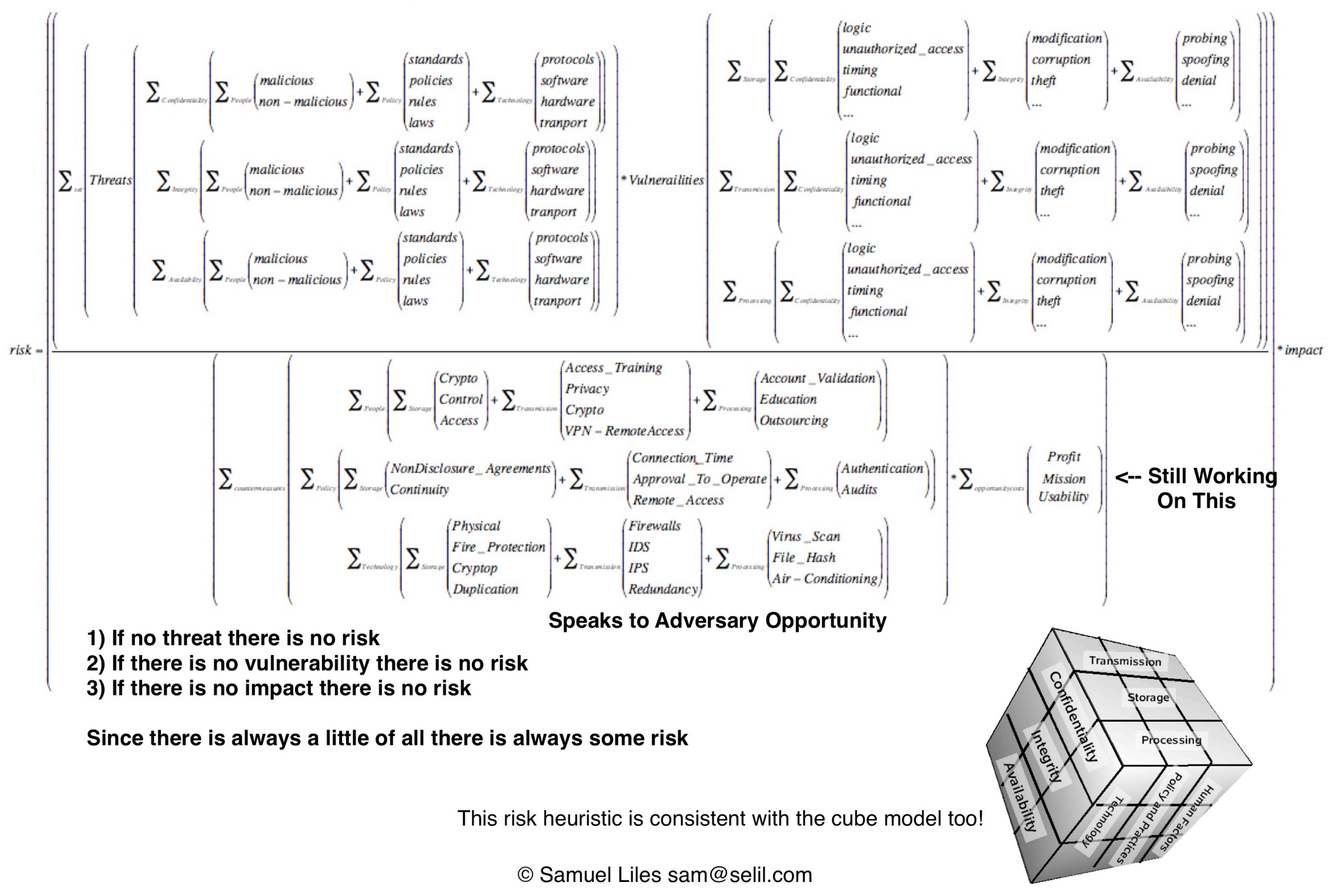
Risk Assessment in an information centric world: Threats, vulnerabilities, countermeasures and impacts (a work in progress)

Samuel Liles


45K Vulnerabilities
2K STIGs
Intelligence
100+ Events
300+ Tools
Ishiwara
Operating Systems
Networks
Databases
History
Policy
OSI 7 Layer, +Human, +Kinetic
Confidentiality, Integrity, or Availability
People, Process, or Technology
Processing, Storage, or Transmission
Results

Speaks to Adversary Motive

Speaks to Adversary Means



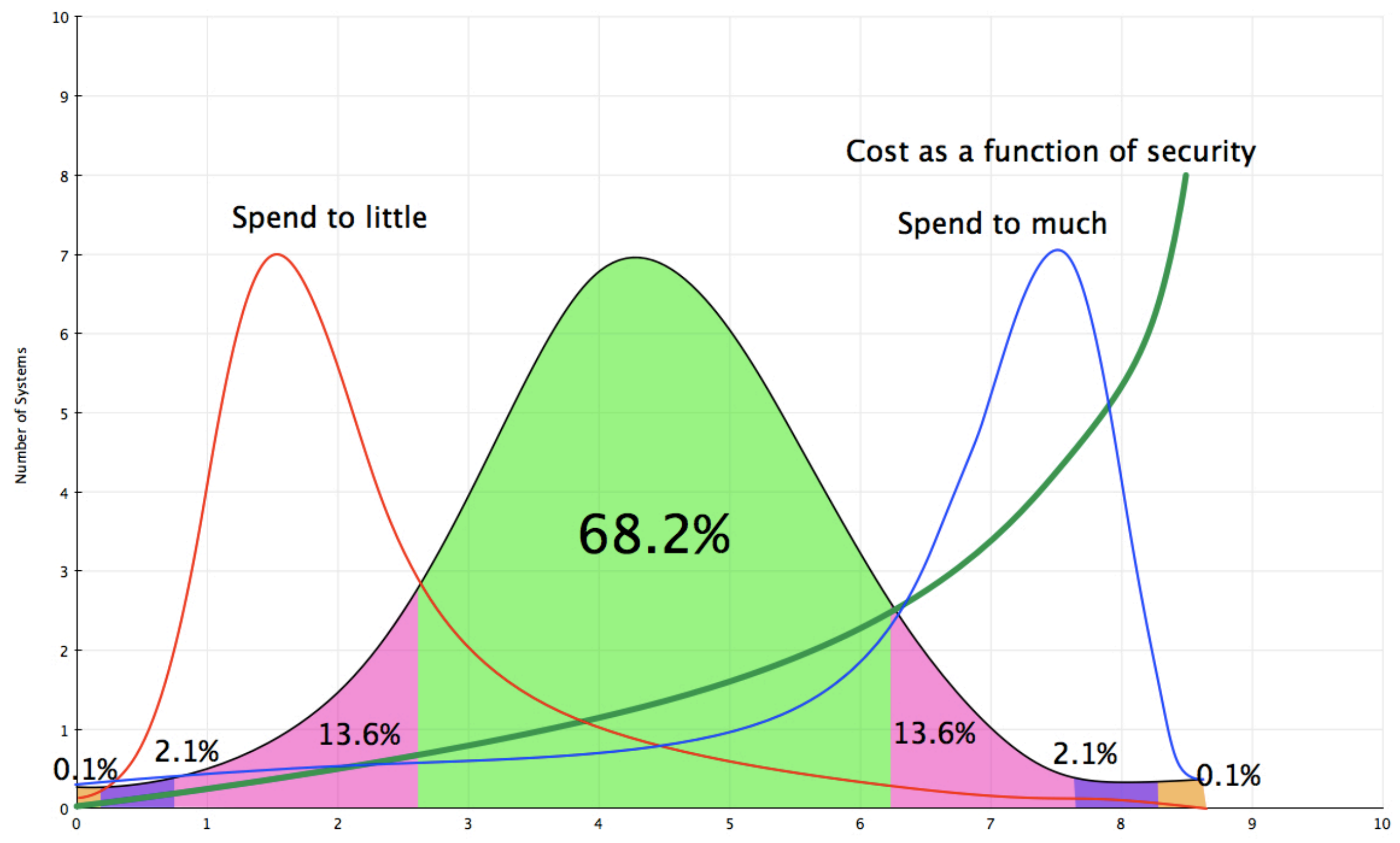
Speaks to Adversary Opportunity

1) If no threat there is no risk
2) If there is no vulnerability there is no risk
3) If there is no impact there is no risk

Since there is always a little of all there is always some risk

This risk heuristic is consistent with the cube model too!

© Samuel Liles sam@selil.com



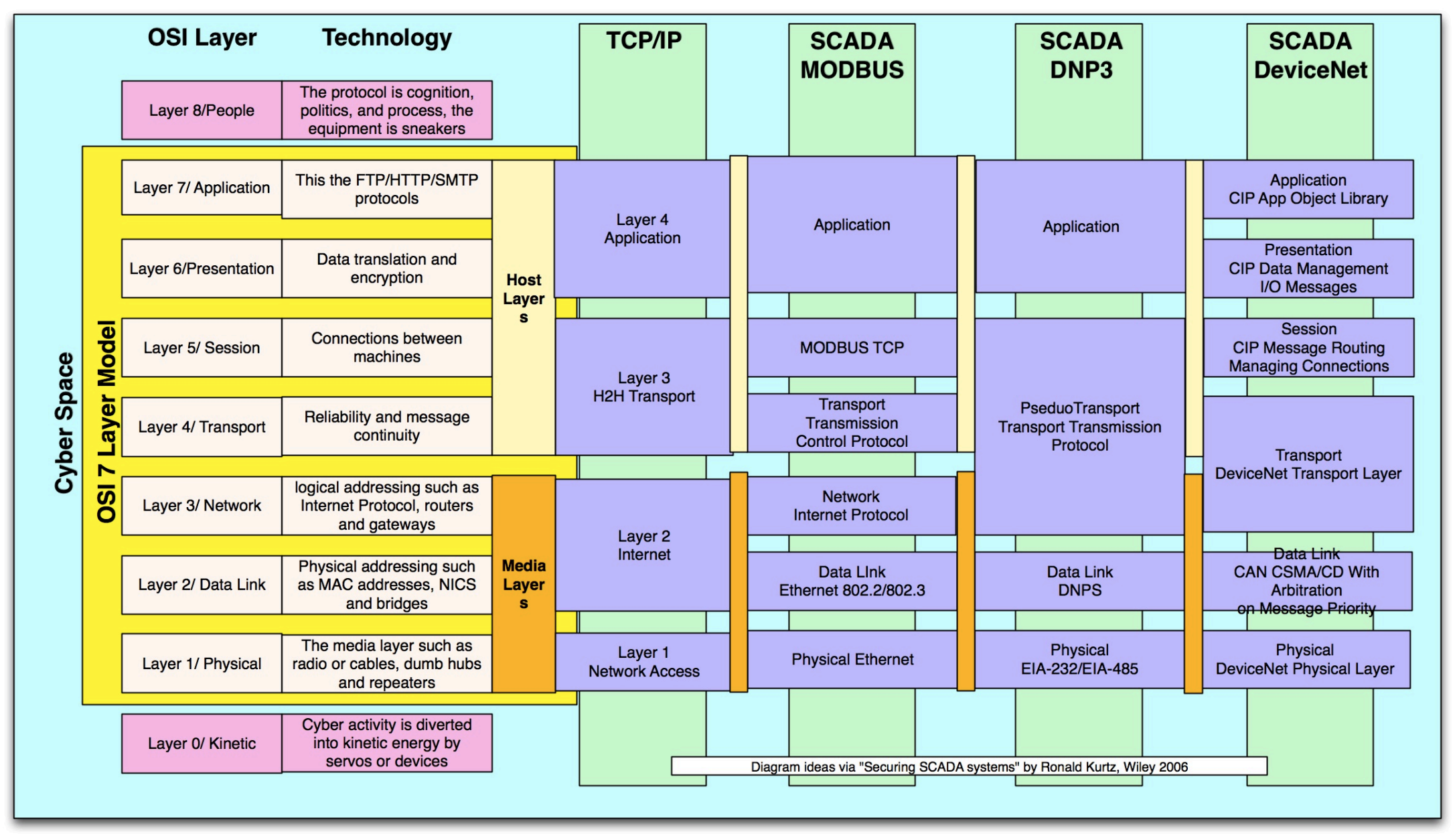
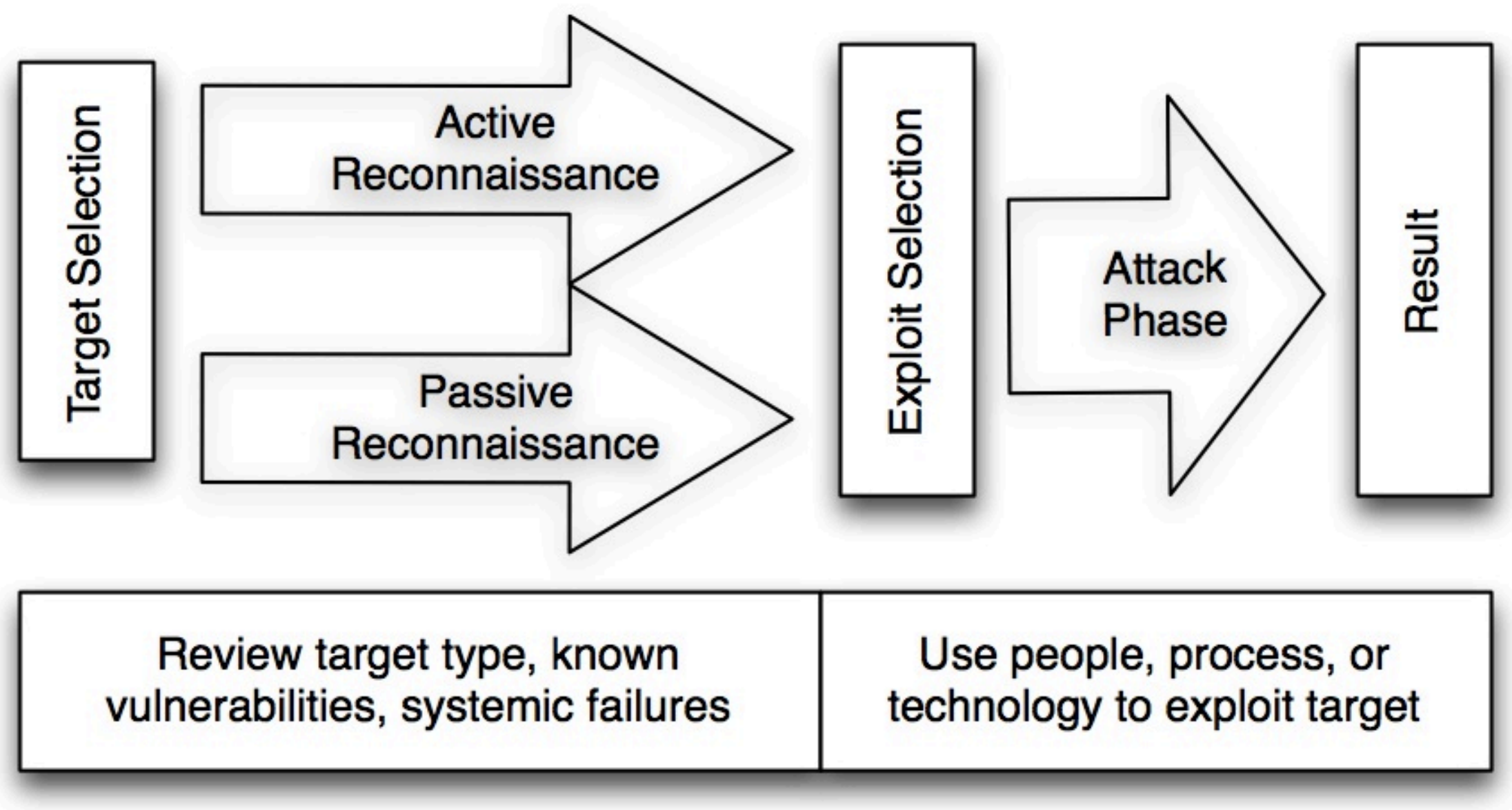
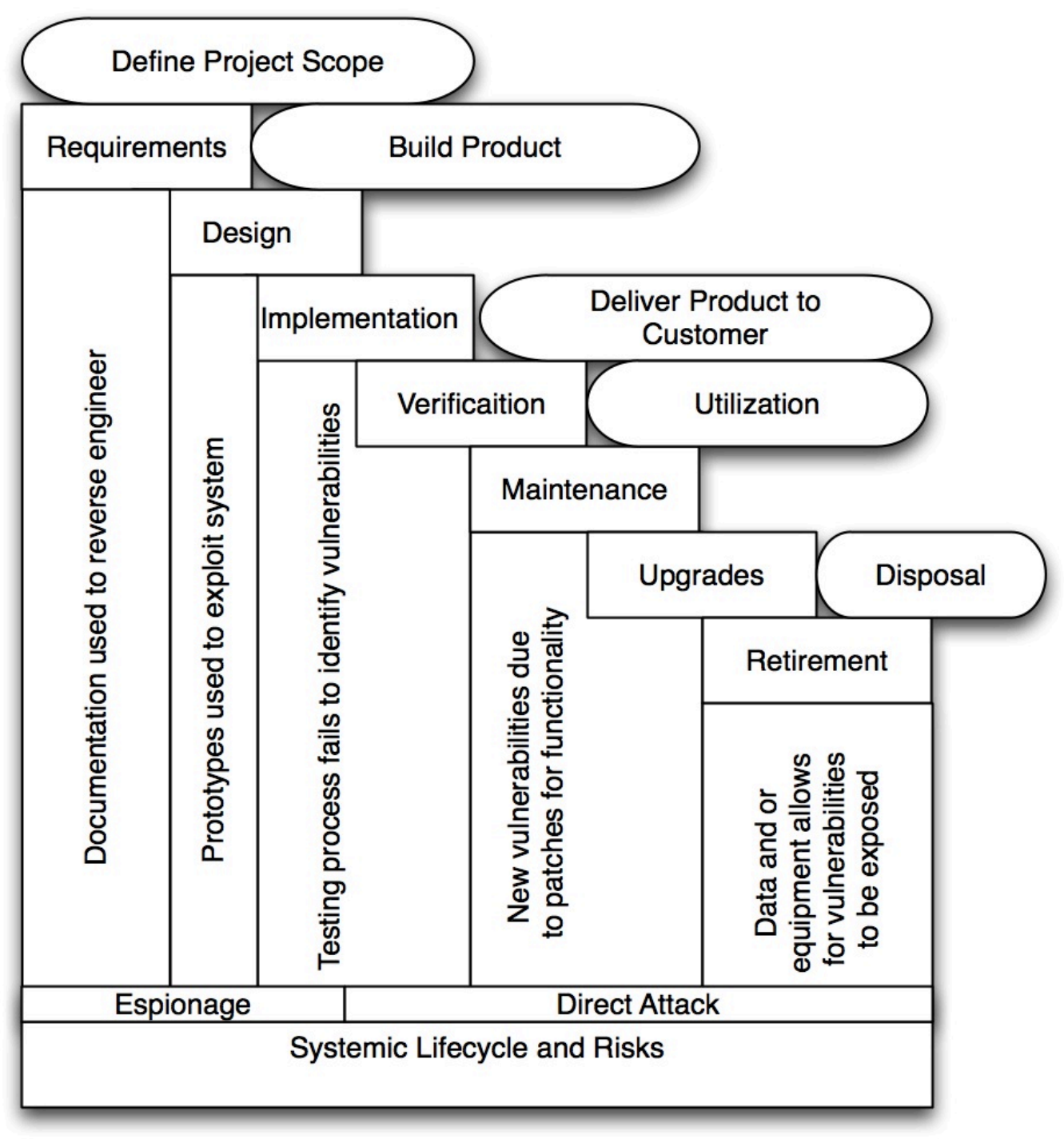

Cyber Space
OSI 7 Layer Model
OSI Layer
Technology
TCP/IP
SCADA MODBUS
SCADA DNP3
SCADA DeviceNet
Layer 8/People
The protocol is cognition, politics, and process, the equipment is sneakers
Layer 7/ Application
This the FTP/HTTP/SMTP protocols
Layer 6/Presentation
Data translation and encryption
Layer 5/ Session
Connections between machines
Layer 4/ Transport
Reliability and message continuity
Layer 3/ Network
logical addressing such as Internet Protocol, routers and gateways
Layer 2/ Data Link
Physical addressing such as MAC addresses, NICS and bridges
Layer 1/ Physical
The media layer such as radio or cables, dumb hubs and repeaters
Layer 0/ Kinetic
Cyber activity is diverted into kinetic energy by servos or devices
Host Layers
Media Layers
Layer 4 Application
Layer 3 H2H Transport
Layer 2 Internet
Layer 1 Network Access
Application
MODBUS TCP
Transport Transmission Control Protocol
Network Internet Protocol
Data LInk Ethernet 802.2/802.3
Physical Ethernet
Application
PseduoTransport Transport Transmission Protocol
Data Link DNPS
Physical EIA-232/EIA-485
Application CIP App Object Library
Presentation CIP Data Management I/O Messages
Session CIP Message Routing Managing Connections
Transport DeviceNet Transport Layer
Data Link CAN CSMA/CD With Arbitration on Message Priority
Physical DeviceNet Physical Layer

Diagram ideas via "Securing SCADA systems" by Ronald Kurtz, Wiley 2006

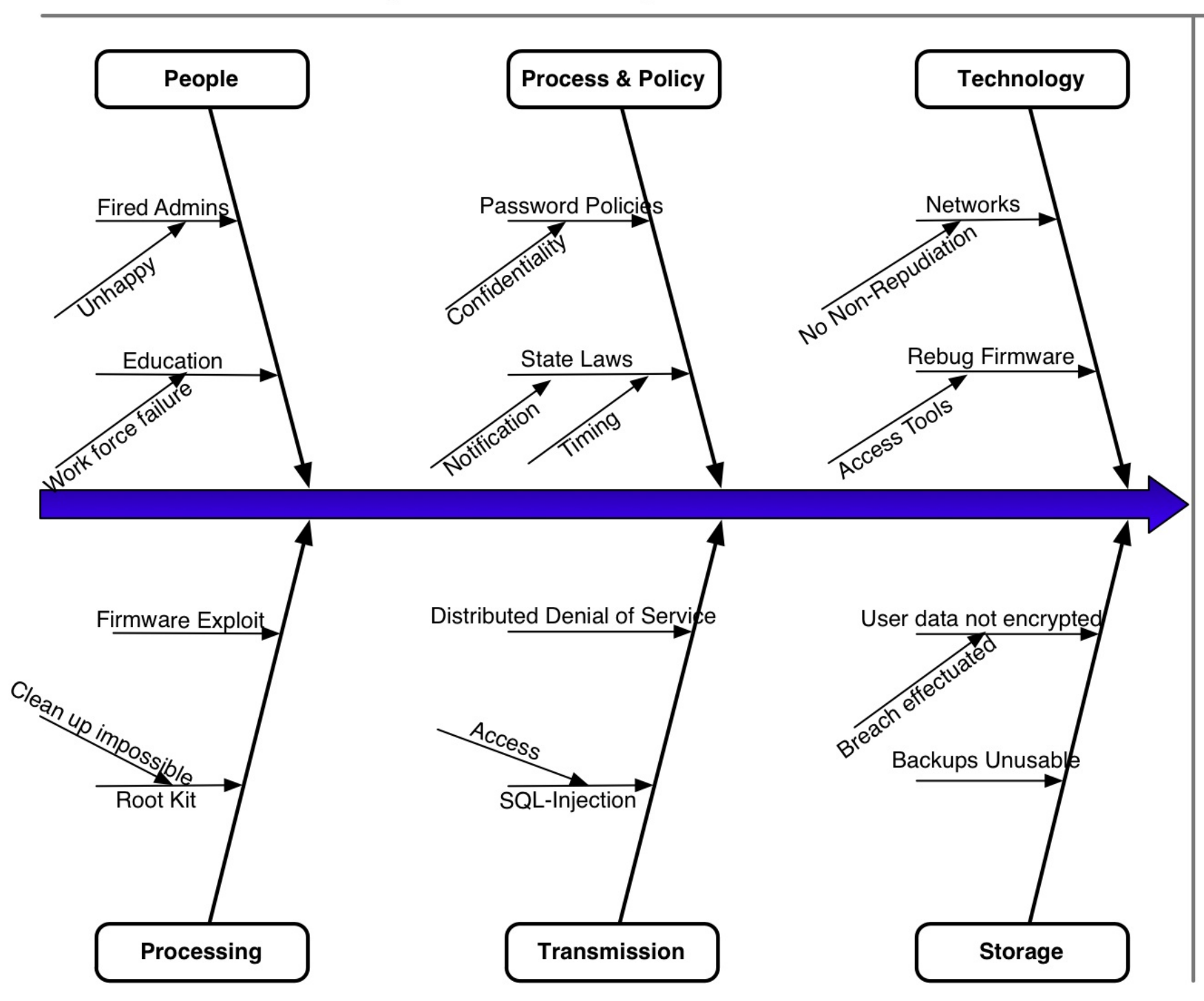


Review target type, known vulnerabilities, systemic failures

Use people, process, or technology to exploit target


Define Project Scope
Requirements
Build Product
Design
Implementation
Deliver Product to Customer
Verificaition
Utilization
Maintenance
Upgrades
Disposal
Retirement
Documentation used to reverse engineer
Prototypes used to exploit system
Testing process fails to identify vulnerabilities
New vulnerabilities due to patches for functionality
Data and or equipment allows for vulnerabilities to be exposed
Espionage
Direct Attack
Systemic Lifecycle and Risks

Sony Data Breach April 6 2011 to ...



Effect

Systems Breach of...

Confidentiality
77 Million peoples PII compromised
Credit cards compromised
Emails leaked

Integrity
Unknown

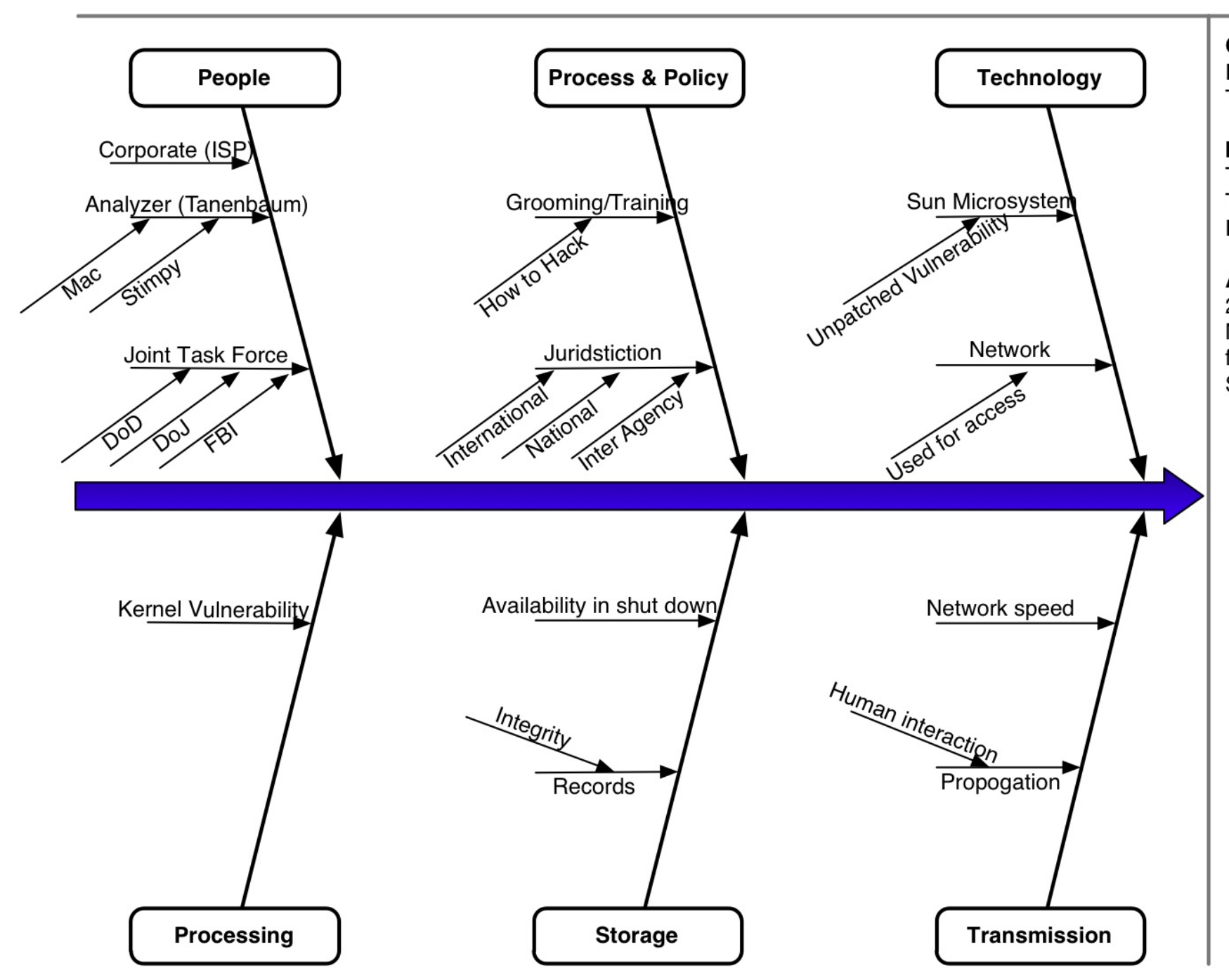
Availability
Various network resources unavailable.

Final toll…
Play Station Network
Sony Corporate
Sony Japan
Sony Online Ent.
Sony Thailand
Sony Greece
Sony Indonesia
Sony Canada

All information based on open source, media reports, and accuracy subject to multitude of factors.

© Samuel Liles

Solar Sunrise Feb 1-26 1998



Effect

Confidentiality
Records and orders exposed
Troop transport exposed

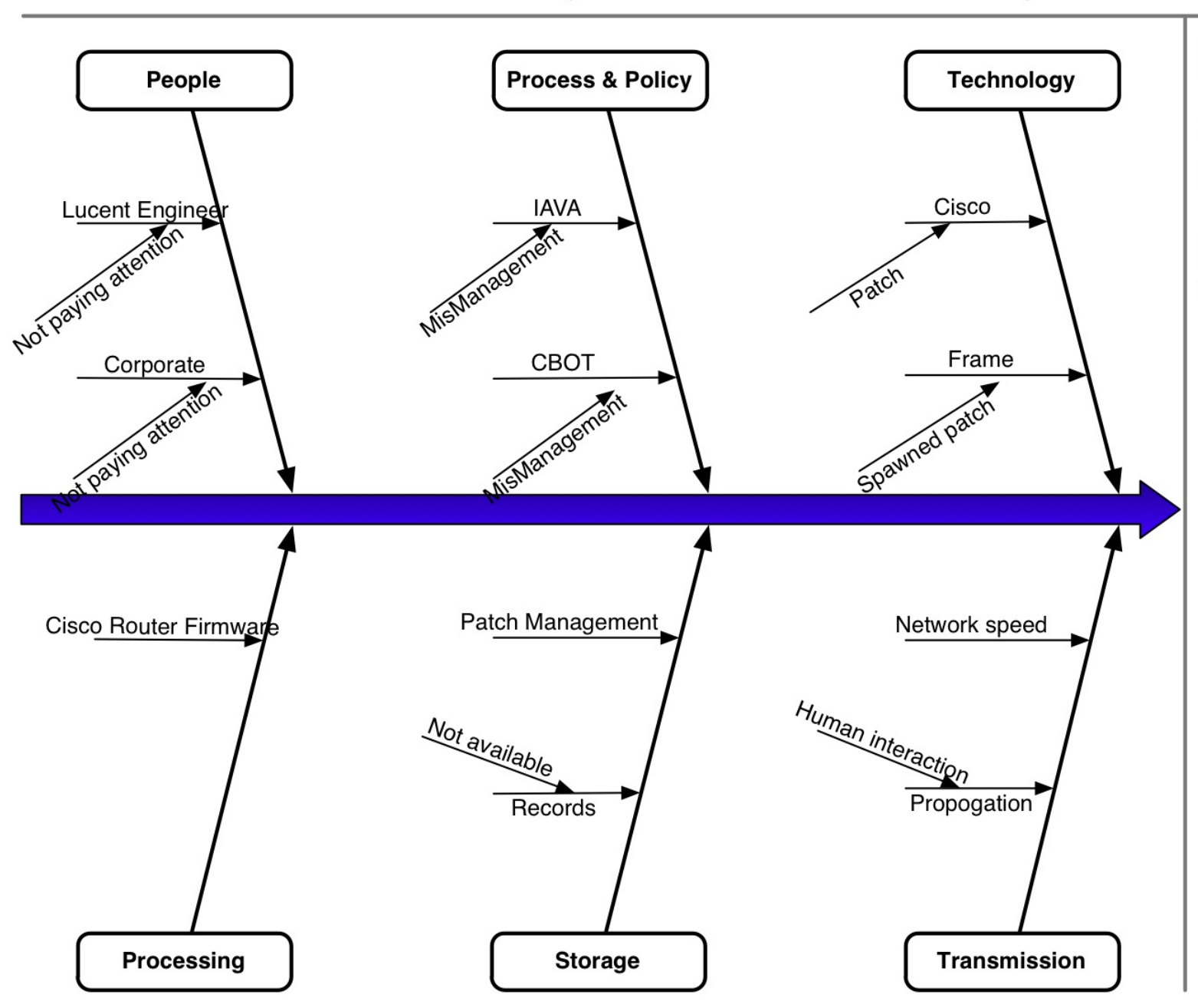
Integrity
Trust in system status failed
Transport orders in jeopardy
Full clean up required

Availability
26 days of intermittent availability
Numerous systems shutdown for forensics
Systems seized for analysis

All information based on open source, media reports, and accuracy subject to multitude of factors.

© Samuel Liles

Causes of Chicago Board of Trade Y2K Outage



Effect

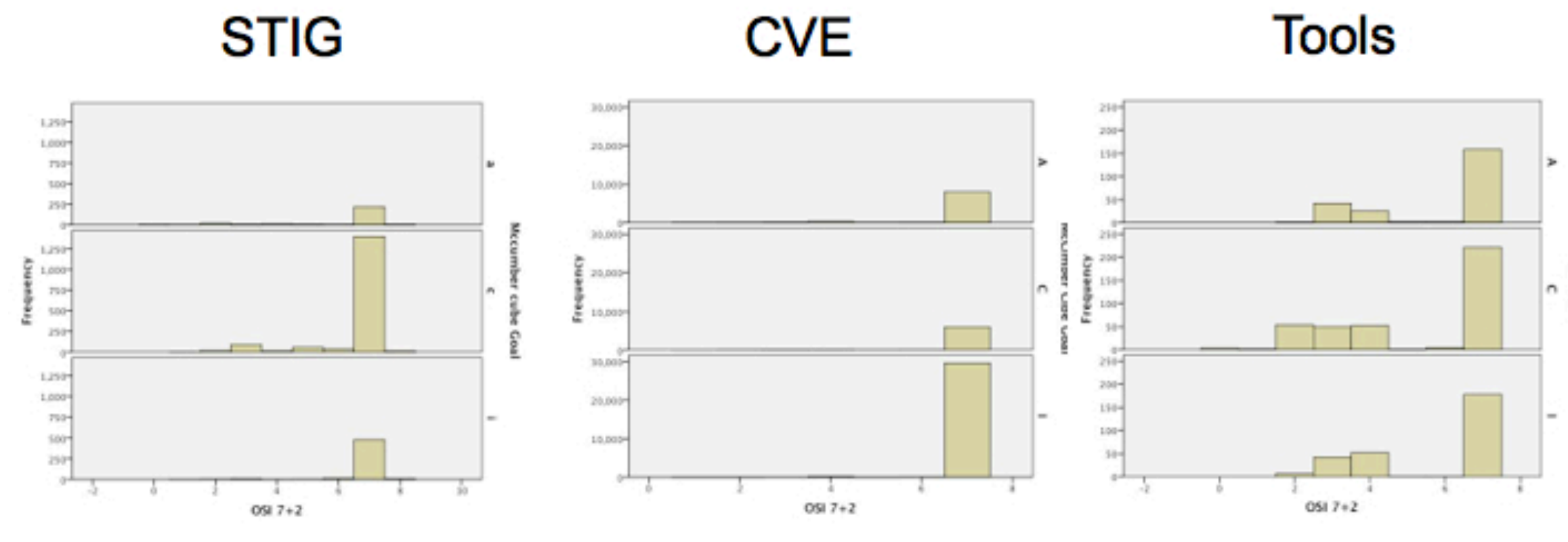
Confidentiality
Unknown

Integrity
Numerous trades had to be rolled back.

Availability
9 days at 60% outage during trade periods

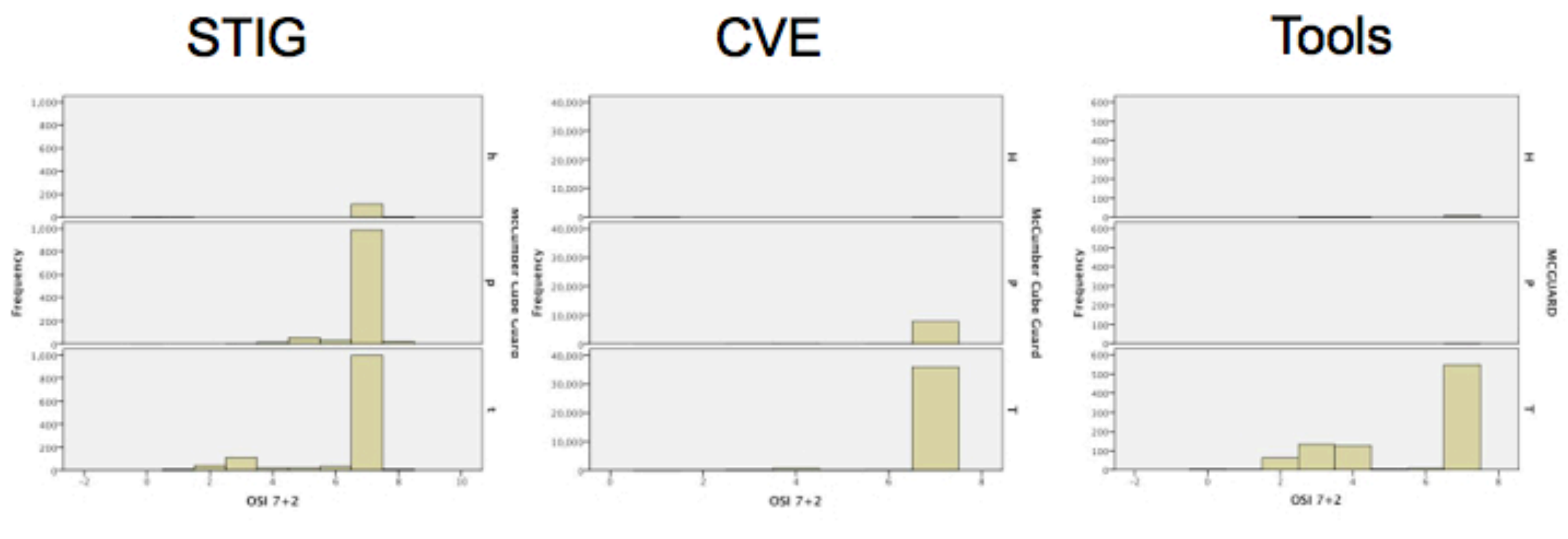
All information based on open source, media reports, and accuracy subject to multitude of factors.

© Samuel Liles



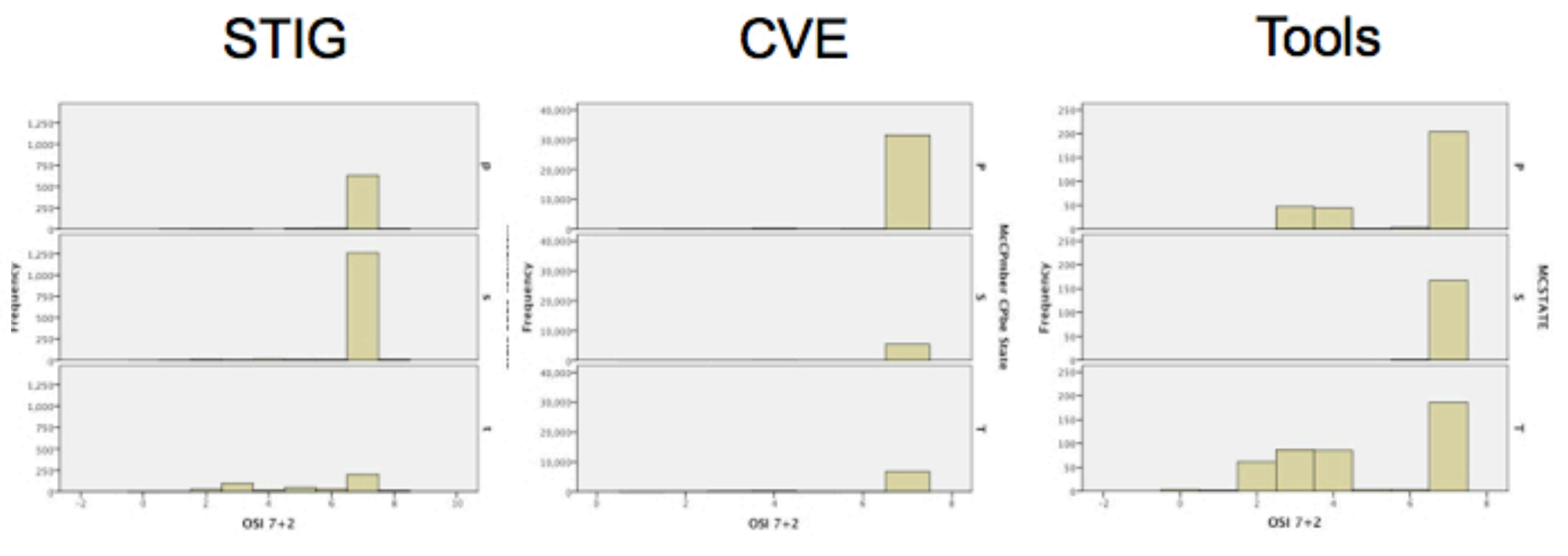
Using confidentiality, integrity, and availability while comparing the various security technical implementation guides against the known vulnerabilities agains the known tools after being put through the taxonomical process

Confidentiality/Integrity/Availability



Using human factors, policy, and technology, while comparing the various security technical implementation guides against the known vulnerabilities against the known tools after being put through the taxonomical process

Human Factors/Policy/Technology



Using processing, storage, and technology, while comparing the various security technical implementation guides against the known vulnerabilities against the known tools after being put through the taxonomical process

Processing/Storage/Transmission

What is this project trying to answer?

How do you do analysis of risk across the domain of information technology using metrics based on empirical evidence for decisions that are evidence based in mitigation and allow for decision processes based on the best information?

CERIAS®

Discovery Park
e-Enterprise Center