Understanding Cyber Defense
A Systems Approach

Instructors

Tom McDermott
Director of Research
Georgia Tech Research Institute
tom.mcdermott@gtri.gatech.edu

Todd Moore
Manager, San Diego Office
Georgia Tech Research Institute
todd.moore@gtri.gatech.edu

Additional Authors

Jeff Moulton
Director, Program Development
Georgia Tech Research Institute
jeff.moulton@gtri.gatech.edu

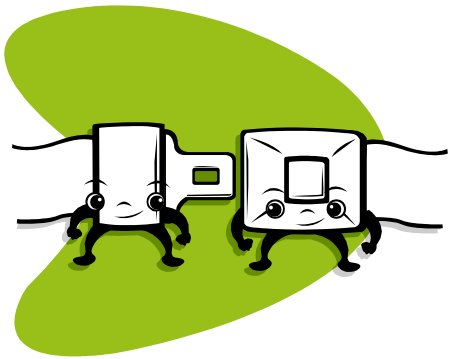
Josh Davis
Senior Research Engineer
Georgia Tech Research Institute
Josh.davis@gtri.gatech.edu

Tutorial Objectives

- Introduce the concept of cyber defense and the need for system engineering approach
- Introduce the cyber threat (attacker) and information assurance (defender)
- Characterize cyber defense as a complex system
- Introduce methods, processes, and tools for managing cyber defense within an enterprise architecture

Agenda

- Introduction to Cyber Security
- Understanding the Threat
- Information Assurance
- Cyberspace as a Complex System
- Enterprise Architecture
- The System Architect
- Example Methods



Cyber is such a perfect prefix. Because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool -- and therefore strange, spooky.

New Yorker Magazine, Dec. 23, 1996

Reference: Wikipedia - Information Age - A Visualization of the various routes through a portion of the Internet.

All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.

William Gibson

NEUROMANCER

What is Cyber Security?

Computer security - protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

Network security - consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources

Information security - protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Cybersecurity - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Reference: http://en.wikipedia.org/wiki/Computer_security, http://en.wikipedia.org/wiki/Information_security, http://en.wikipedia.org/wiki/Network_security, http://www.merriam-webster.com/dictionary/cybersecurity

Current State, Unattributed Quotes

- “The state of cyber security today is a complete failure…If you haven’t been hacked you have nothing of interest to steal”
- “fundamental trust models in cyberspace are broken; there is no technology out there today that reflects trust; 100 years from now we will realize we were in a lawless state”
- “why do we lack systems understanding, holistic design principles, risk management, and training in our enterprise systems?”
- “we are our worst enemies…the problem is too huge…we cannot conceptualize it, cannot worry about it”
- “it’s going to take a ‘BP oil spill of data’ event to wake us up”

Current State is Rapidly Evolving & Expanding

- Hacker (1960's)
  - A person who enjoys exploring the details of programmable systems and stretching their capabilities
- "WarGames" (1983)
  - A young hacker starts the countdown to World War 3.
- Computer Viruses (1980's)
  - Tool era - Self-replication & connectivity
- Hacktivism (1990's)
  - WANK Worm … to Anonymous & Lulz
- Cyber Criminals (2000's)
  - Financial theft, illicit trade
- Cyber Espionage (last decade)
  - Characterized by persistence
- Cyber Kinetic Attacks (emerging)
  - Primarily nation-state based, target physical systems

Current State is Rapidly Evolving

- Remarkable change in attack motivation from our IT Systems to our Enterprises
- Around 2005, saw attacks shift from individual IT systems to commercial enterprises
  - Unprecedented transfer of wealth, not just IP but also enterprise strategies
  - Organized crime and nation-state involvement
- Key threat shift: preparation and patience
  - Not hacking – normal IT tradecraft used, but the technology is mainstream
  - Espionage: reconnaissance, exfiltration, exploitation, profit
- New paradigms – “we have no idea what’s out there”

This is a Systems Problem

- No longer just an information technology issue
- Need to move from a vulnerability-centric model to a threat-centric model
- Need to move from a tool-centric perspective to a value-centric perspective
- Organizations must have a strategic cyber defense plan that drives their business approach
- The strategic plan must be threat-driven with targeted protection practices

This is a Complex Adaptive System

"everyone has a plan until they are punched in the face" (Mike Tyson)

- Threats and enterprise technologies are rapidly changing
- Cyber protection frameworks are dynamic and require constant reassessment

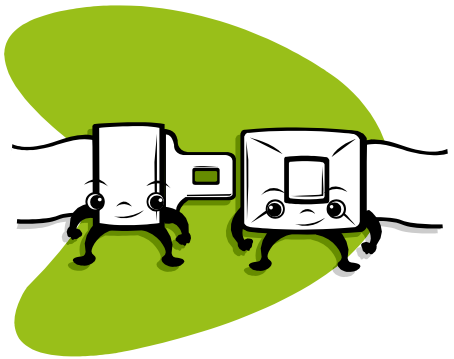
"our dependency is scary"

"protection is futile, resilience is the key"

- IT Systems, business practices, and social systems are completely intertwined
- Do you understand how complex this is?

Agenda

- Introduction to Cyber Security
- Understanding the Threat
- Information Assurance
- Cyberspace as a Complex System
- Enterprise Architecture
- The System Architect
- Example Methods



Assessment Exercise

- Write down the answers to these questions for your organization:
  1. What is the sensitive information in your organization?
  2. Where is it?
  3. Who has access to it?
  4. Who you know and trust in your organization?
  5. How do you insure against loss of sensitive information?

What

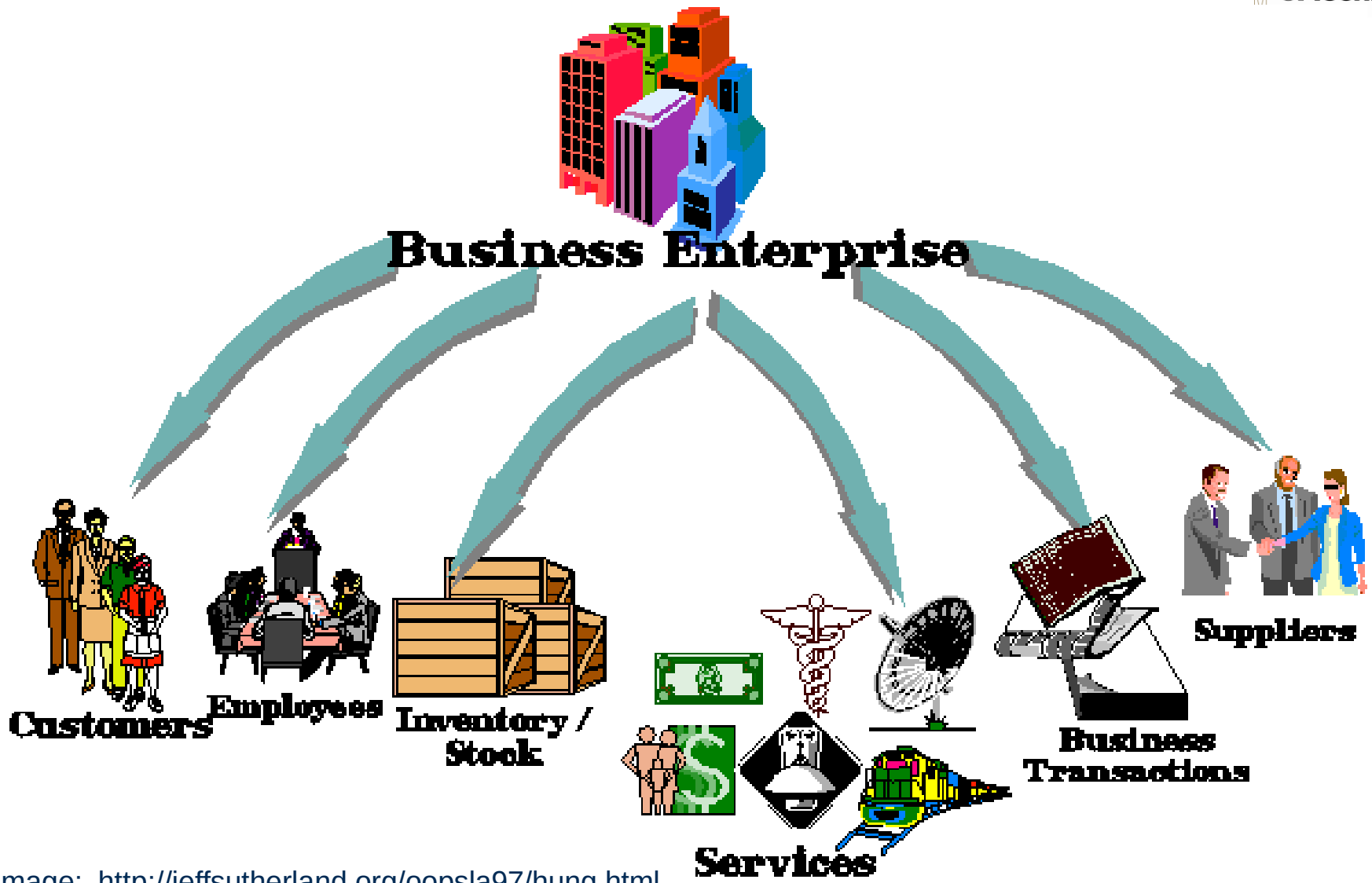
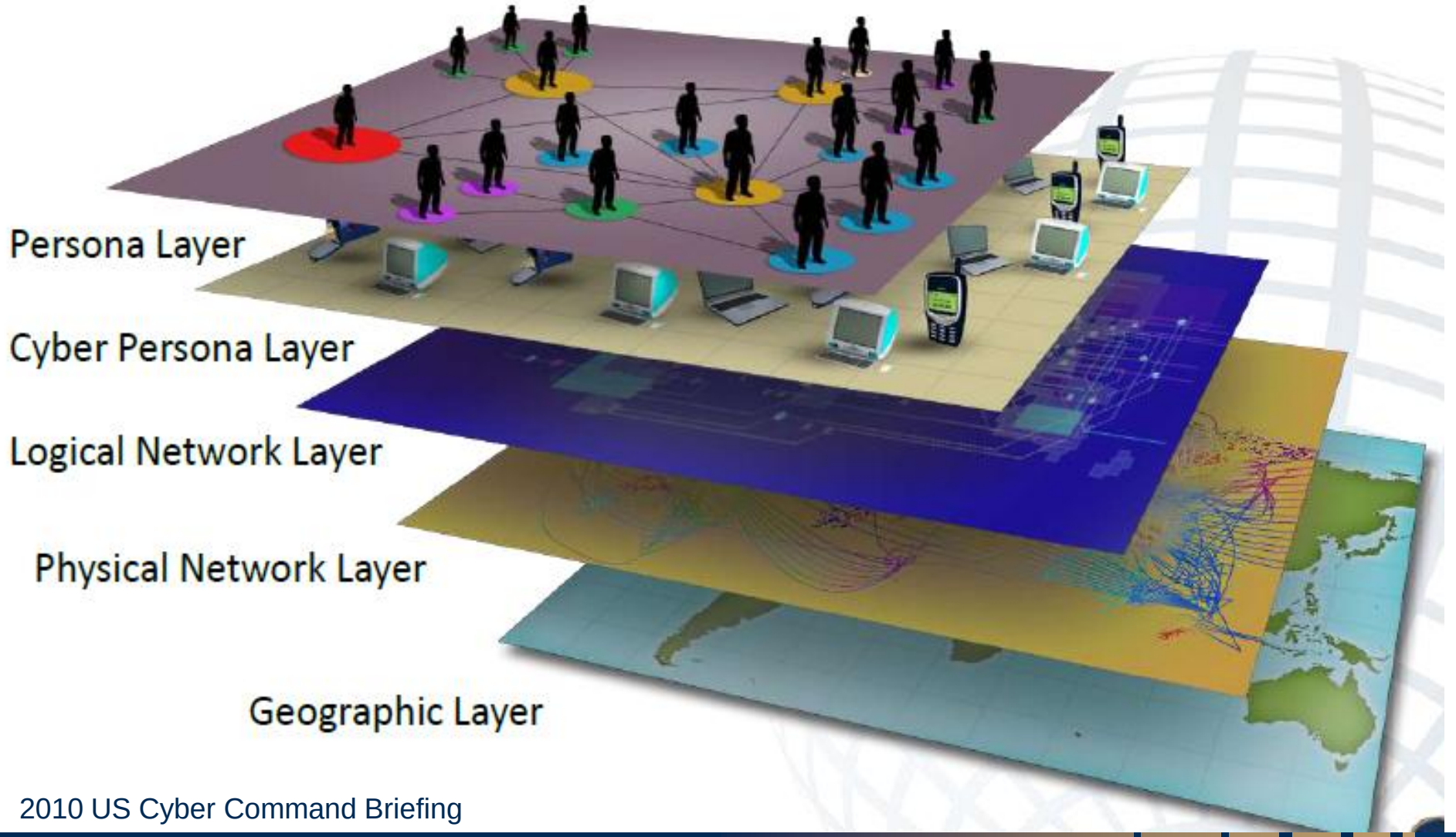


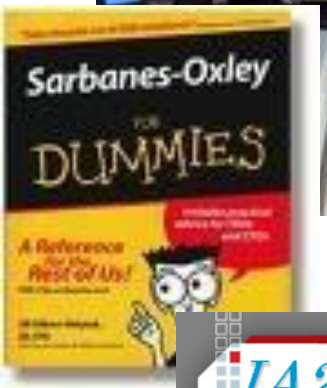
Image: http://jeffsutherland.org/oopsla97/hung.html

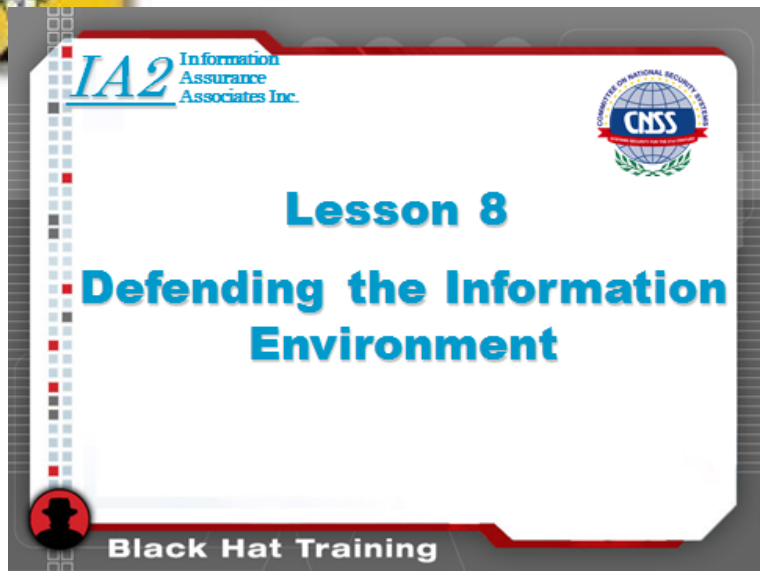
Who and Where



2010 US Cyber Command Briefing

How





US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Welcome to the US-CERT Incident Reporting System

What is an incident?
A good but fairly general definition of an incident is *The act of violating an explicit or implied security policy*. Unfortunately, this definition relies on the existence of a security policy that, while generally understood, varies among organizations.

For the federal government, an incident, defined by NIST Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Federal incident reporting guidelines, including definitions and reporting timeframes can be found at http://www.us-cert.gov/federal/reportingRequirements.html.

In general, types of activity that are commonly recognized as being in violation of a typical security policy include but are not limited to

- attempts (either failed or successful) to gain unauthorized access to a system or its data, including PII related incidents (link to the below description)
- unwanted disruption or denial of service
- the unauthorized use of a system for processing or storing data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

We encourage you to report any activities that you feel meet the criteria for an incident. Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

Using the US-CERT Incident Reporting System

In order for us to respond appropriately, please answer the questions as completely and accurately as possible. Questions that must be answered are labeled "Required". As always, we will protect your sensitive information. This web site uses Secure Sockets Layer (SSL) to provide secure communications. Your browser must allow at least 40-bit encryption. This method of communication is much more secure than unencrypted email.

Section: Reporter's Contact Information

First Name *(Required)*
Last Name *(Required)*
Email Address *(Required)*
Please re-enter for verification
Telephone number *(Required)*
Are you reporting as part of an Information Sharing and Analysis Center (ISAC)? No, this is not an ISAC report
What type of organization is reporting this incident? *(Required)* Please select
What is the impact to the reporting organization? *(Required)* Please select
What type of followup action are you requesting at this time? *(Required)* Please select
Describe the current status or resolution of this incident. *(Required)* Please select
From what time zone are you making this report? *(Required)* Please select a time zone
What is the approx time the incident started? (localtime) October 16 , 2011 : 18 : 56
When was this incident detected? (localtime) October 16 , 2011 : 18 : 56

Section: Incident Details

Please provide a short description of the incident and impact *(Required)*

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular

Sickos can wreak death

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks

scarier," Yabenson said.

"Soon it will be sold to terrori cults and fanatical religious-frin groups.

"Instead of blowing up a sing plane, these groups will be able patch into the central computer o large airline and blow up hundre of planes at once.

"And worse, this e-mail bon program will eventually find its w

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon

November 29, 2010 4:40 PM

PRINT TEXT

Iran Confirms Stuxnet Worm Halted Centrifuges

By **CBSNews**

Georgia Institute of Technology

1 Comment Have Your Say | **Email Story** Send to a Friend | **Share This** Tell Your Friends | **Tweet This** Tweet This | **More** Share It

(CBS/AP) Iran's president has confirmed for the first time that a computer worm affected centrifuges in the country's uranium enrichment program.

Iran has previously denied the Stuxnet worm, which experts say is calibrated to destroy centrifuges, had caused any damage, saying they uncovered it before it could have any effect.

But President Mahmoud Ahmadinejad has said it "managed to create problems for a limited number of our centrifuges." Speaking to a press conference Monday, he said the problems were resolved.

Earlier in November, U.N. inspectors found Iran's enrichment program temporarily shut down, according to a recent report by the U.N. nuclear watchdog. The extent and cause of the shutdown were not known, but speculation fell on Stuxnet.

The finding was contained in a report from the International Atomic Energy Agency for the U.N. Security Council and the 35 IAEA board member nations.

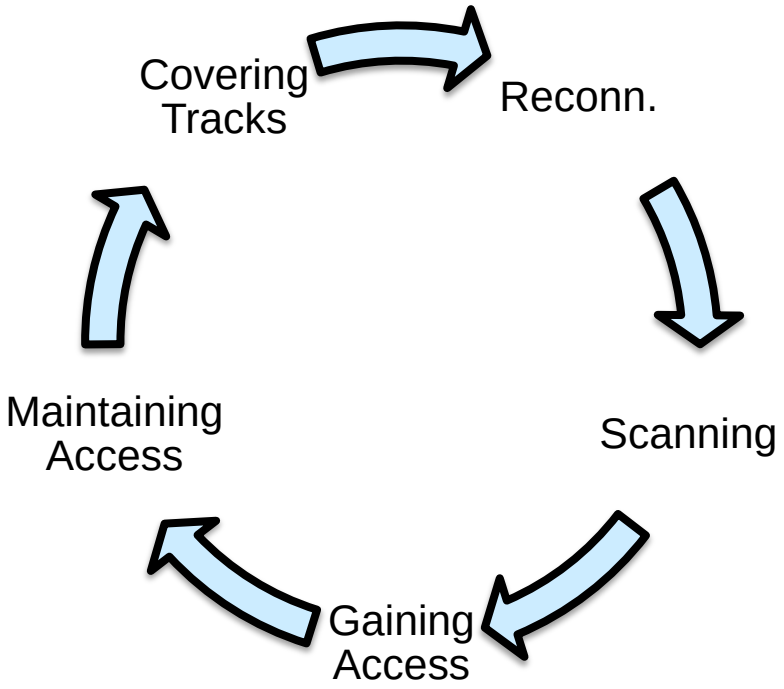
Diplomats who spoke to the Associated Press that week said they did not know why the thousands of centrifuges stopped turning out material that Iran says it needs to fuel a future network of nuclear reactors.

Speculation has focused on the Stuxnet worm, which cyber experts have identified as configured to damage centrifuges.

Vice President Ali Akbar Salehi initially said details about the virus became known only after Iran's "enemies failed to achieve their goals."

Hacking/Cracking

- In computer security and everyday language, a hacker is someone who breaks into computers and computer networks.
- Hackers may be motivated by a multitude of reasons, including profit, protest, or because of the challenge.
- The subculture that has evolved around hackers is often referred to as the computer underground but it is now an open community.



Malware

SECURELIST

Internet threat level: 1

Read us on facebook

Threats | Analysis | Blog | Descriptions | Glossary

Home → Analysis → 03 Mar 2011 → Monthly Malware Statistics, February 2011

Monthly Malware Statistics, February 2011

Share Print

February in figures

The following statistics were compiled in February using data from computers running Kaspersky Lab products:

- 228,649,852 network attacks blocked;
- 70,465,949 attempted web-borne infections prevented;
- 252,187,961 malicious programs detected and neutralized on users' computers;
- 75,748,743 heuristic verdicts registered

Cybercriminals perfecting drive-by attacks

February saw considerable growth in the use of Cascading Style Sheets (CSS) that contain partial data for script downloaders, a new method for spreading malware that makes it much harder for many antivirus solutions to detect malicious scripts. This method is currently being used in the majority of drive-by download attacks and allows cybercriminals to download exploits to users' machines without those exploits being detected.

Drive-by attacks using this method involve redirecting users from an infected site to a page containing CSS data and a malicious script downloader, usually with the help of iFrame. Three infected pages of this type were among the Top 20 most malicious programs detected on the Internet in February: Trojan-

Author

Vyacheslav Zakorzhevsky

» All analysis articles

Analysis

» Monthly Malware Statistics: August 2011
» IT Threat Evolution: Q2 2011
» Monthly Malware Statistics: July 2011
» Monthly Malware Statistics, June 2011
» IT Threat Evolution for Q1-2011

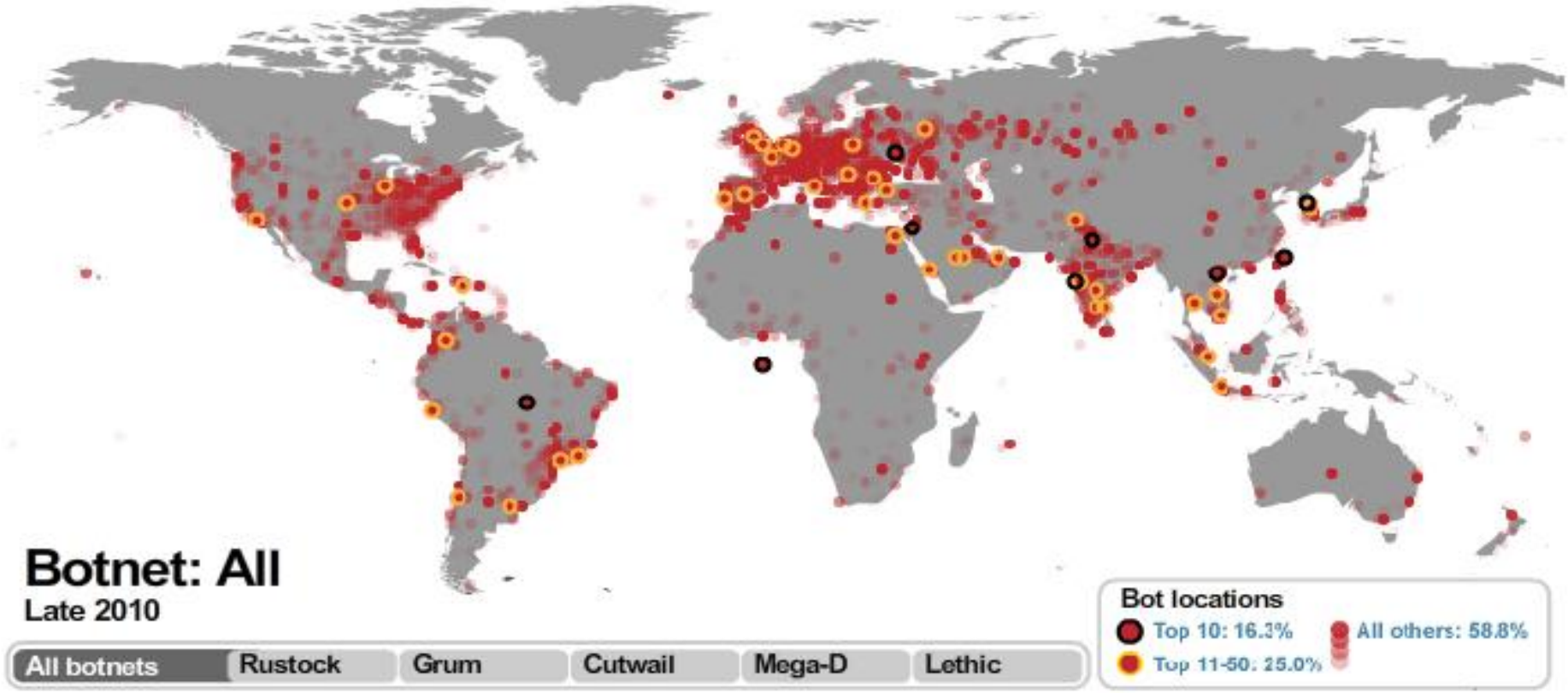
Reference: http://www.securelist.com/en/analysis/204792185/Monthly_Malware_Statistics_July_2011

Denial of Service

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.
- Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

Reference: http://en.wikipedia.org/wiki/Denial-of-service_attack

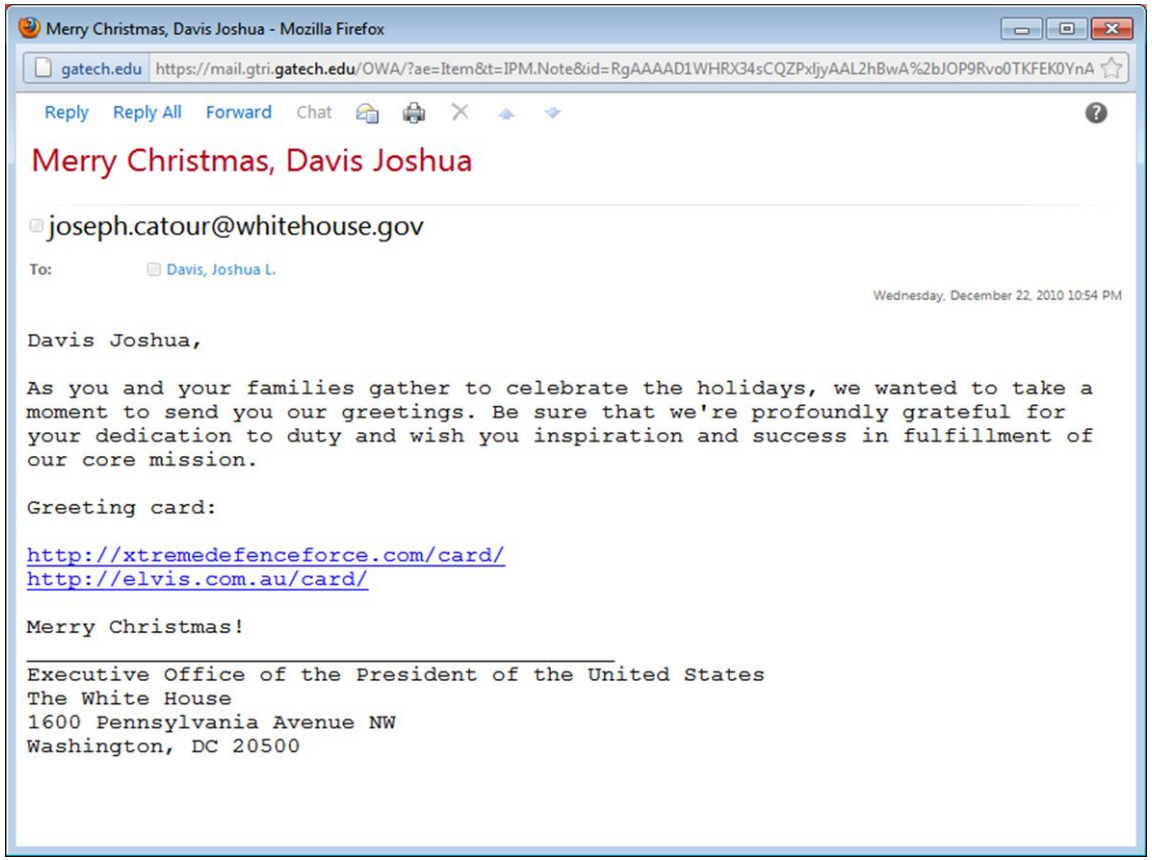
Botnets



Reference: http://www.symanteccloud.com/en/gb/globalthreats/threatmaps/botnets

Phishing

- Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.



Password and Crypto Cracking

- Off-the-shelf tools - Proprietary, Freeware, and Open Source Software
- Approaches – brute-force, dictionary, rainbow tables, etc.
- Passwords “stored” on server, cache, etc.
- Length can impact vulnerability
- Password approach similarities
- Graphics Processing Units

CNN Tech

SEARCH

POWERED BY Google

cs | Justice | Entertainment | Tech | Health | Living | Travel | Opinion | iReport | Money › | Sports ›

WEBSITES

How to create a 'super password'

August 20, 2010 | By John D. Sutter, CNN

Share | Twitter | Email

Recommend | 3,741 people recommend this. Be the first of your friends.

Say goodbye to those wimpy, eight-letter passwords.

The 12-character era of online security is upon us, according to a report published this week by the Georgia Institute of Technology.

The researchers used clusters of graphics cards to crack eight-character passwords in less than two hours.

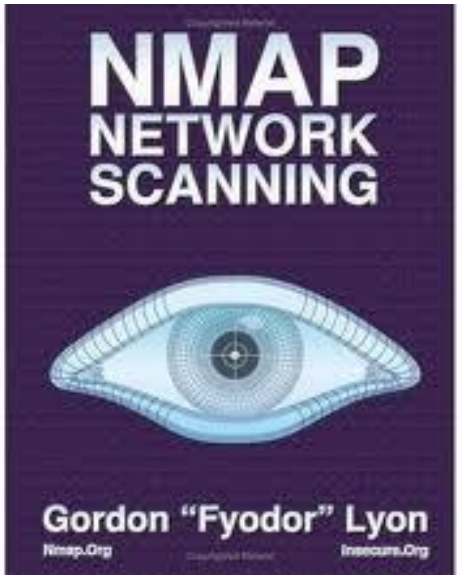
But when the researchers applied that same processing power to 12-character passwords, they found it would take 17,134 years to make them snap.

Want to keep your online data secure? You may need a 12-character password, researchers say.

"The length of your password in some cases can dictate the vulnerability," said Joshua Davis, a research scientist at the Georgia Tech Research Institute.

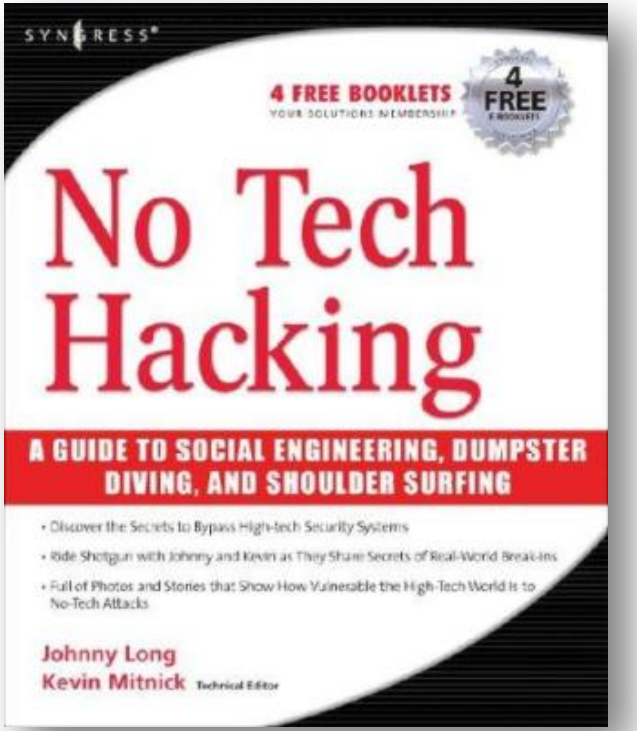
Monitoring, Sniffing, and Scanning

- Reconn/Scanning
- Footprinting
- Fingerprinting
- “Google Hacking”
- Off-the-Shelf
  - Freeware
  - Open Source Software



Social Engineering

- Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.
- "Social engineering" as an act of psychological manipulation was popularized by hacker-turned-consultant Kevin Mitnick. The term had previously been associated with the social sciences, but its usage has caught on among computer professionals.



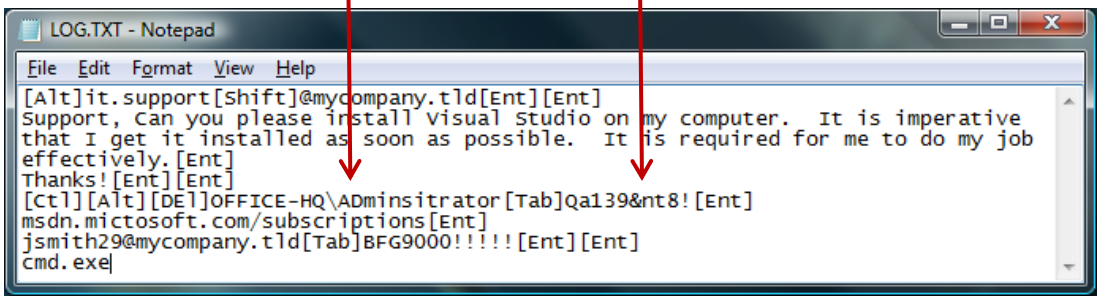
Reference: http://en.wikipedia.org/wiki/Social_engineering_(security)#Definitions

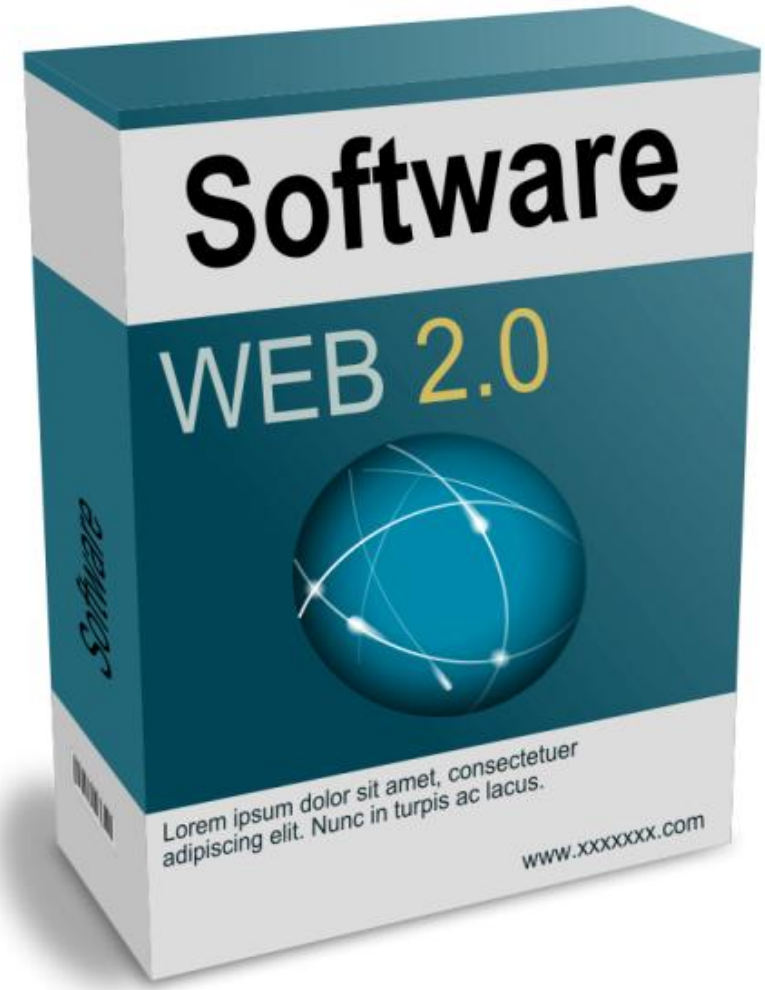
Social Engineering: the Insider Threat

- Start Simple: Use a hardware based keylogger
  - Provided physical access

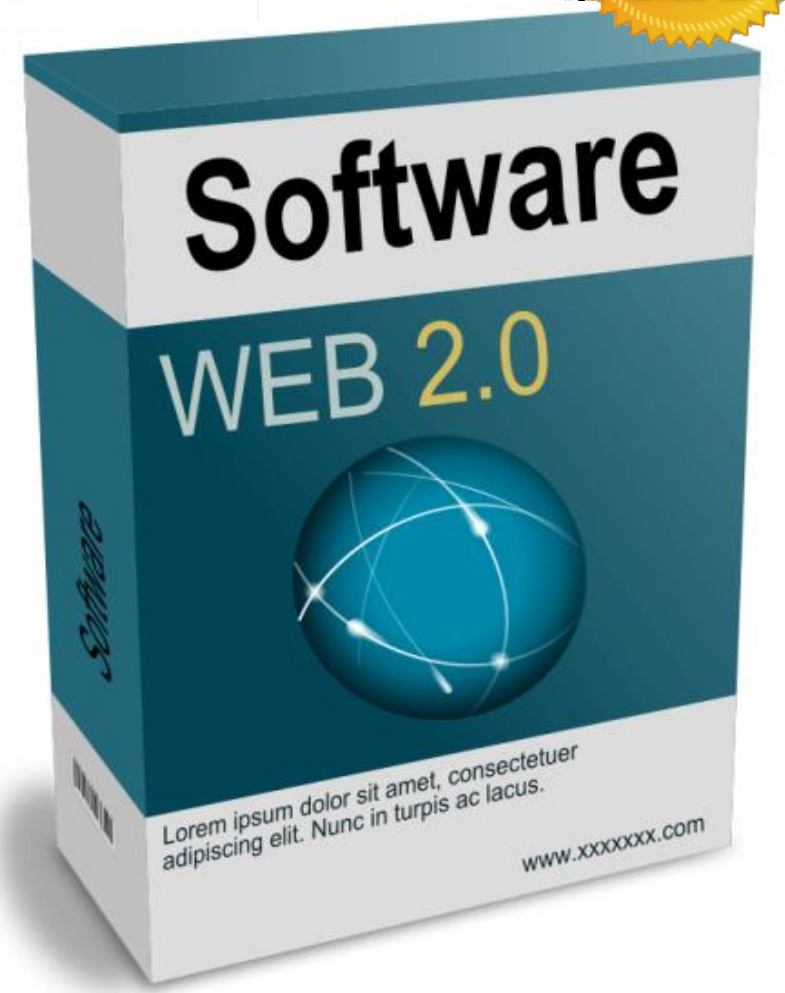
- Install Keylogger
- Call IT for help – Have something fixed/installed
- Collect their credentials
- Enjoy!

Username / Password





amazon.com



amazon.com

Reference: http://www.openclipart.org/detail/65629

amazon.com

amazon.com

Impact on the Individual

- Generally not “security” aware - consequences not immediate
- “Too many accounts and too many passwords”
- Information overload
- Vulnerable to identity, credit card, and credential theft
- “Good” security expensive
- Individuals remain the Employer’s “vulnerable vector”

Impact on Industry

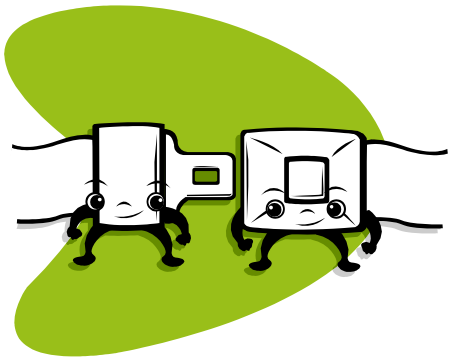
- Legacy - latching on security
- IP Enabling - latching on “cyber”
- “Good” security expensive
- Dearth of talent
- Security posture changes daily++
- Owns/controls critical infrastructure

Impact on Government

- Cyber Warfare
- Legacy - latching on security
- IP Enabling - latching on “cyber”
- Dearth of talent
- “Good” security expensive
- “Inexpensive” intelligence gathering
- Pace of innovation, acquisitions, and policies
- Doesn’t own/control critical infrastructure

Agenda

- Introduction to Cyber Security
- Understanding the Threat
- Information Assurance
- Cyberspace as a Complex System
- Enterprise Architecture
- The System Architect
- Example Methods



Information Assurance (IA)

- Measures taken to protect and defend sensitive information from an adversaries efforts to deny, destroy, degrade or disrupt information or information systems.
- Measures taken to ensure that information is available, reliable, defendable and verifiable.
- Measures taken to ensure that information and information systems implement requisite protection, detection, and reaction capabilities.

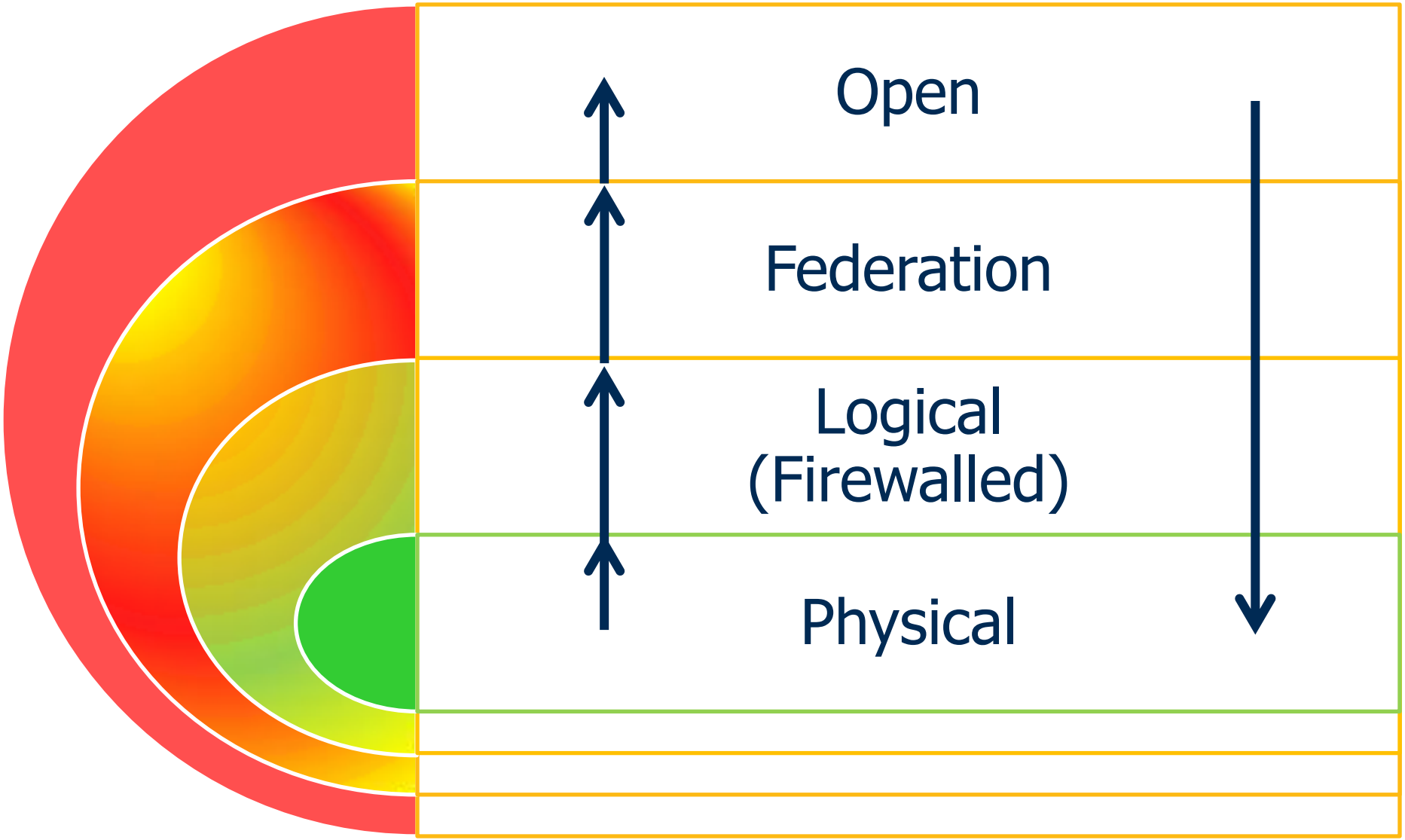
Information Operations

- Information systems process sensitive data in a highly interactive/interconnected/interdependent environment.
- Information systems must interact with other enterprise systems, private and public networks and commercial providers.
- The complexity of distributed computing environments present significant operational and security challenges.

Information Assurance Goals

- Provide end-to-end protection of the information flow.
- Protect information systems from malicious or unauthorized activity.
- Provide situational awareness and command-and-control of information systems.
- Improve operability and interoperability though the introduction of secure processes and procedures.

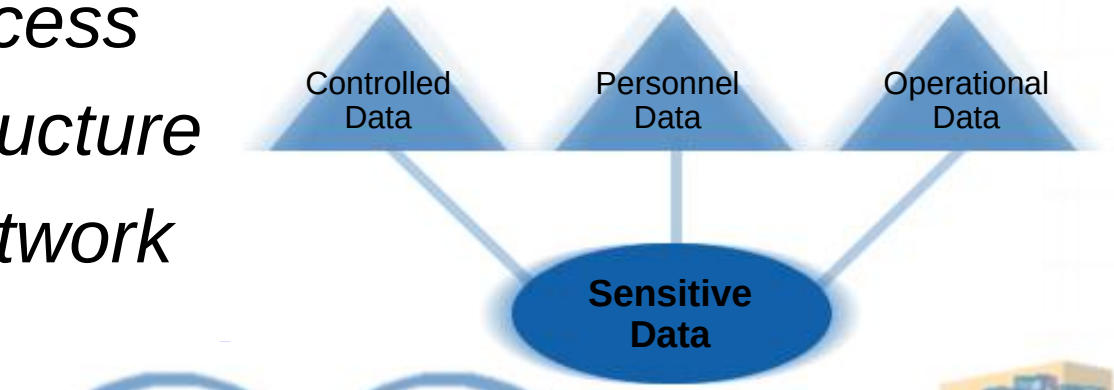
Today's Information Access View

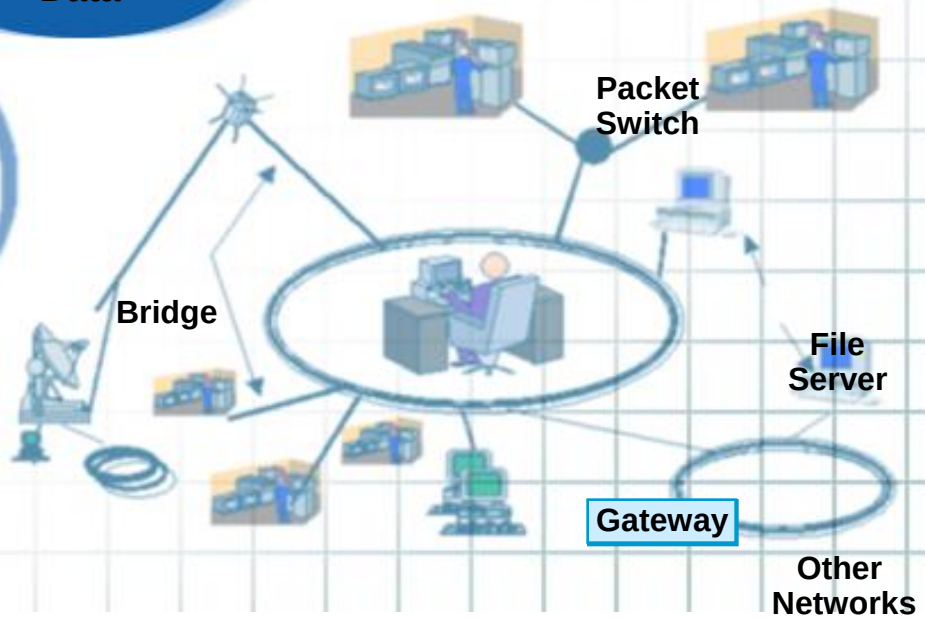


When Information Becomes Digital Data

Concerned with:

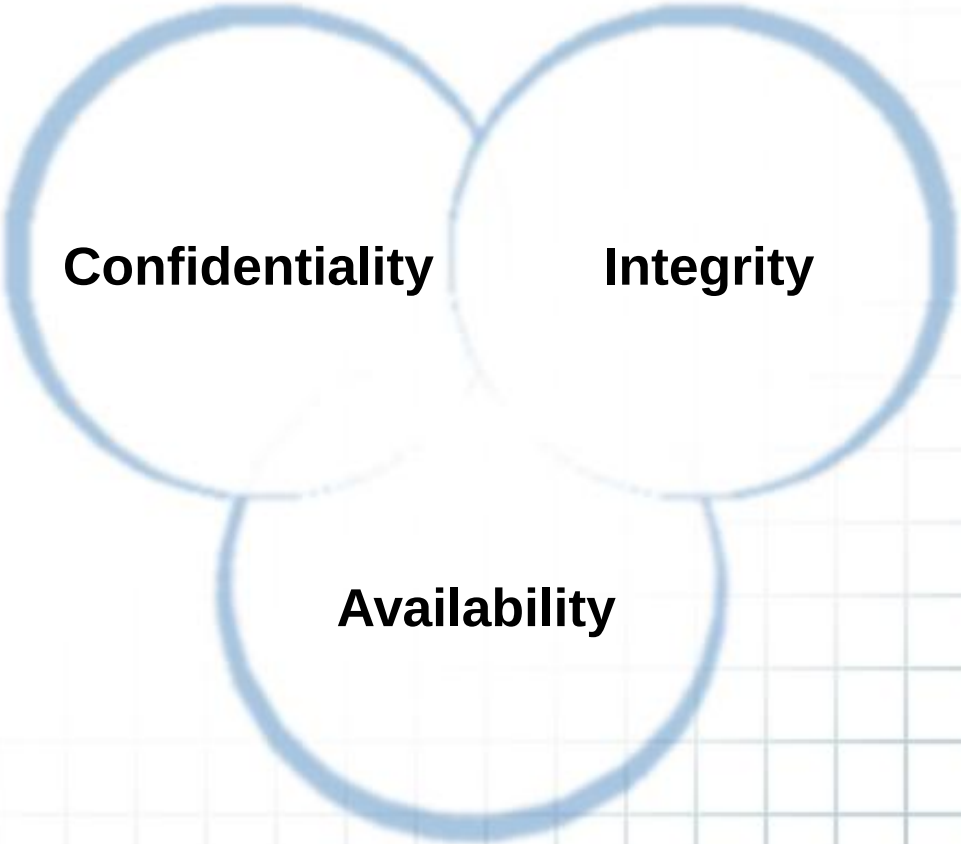
- Data *Access*
- Data *Structure*
- Data *Network*





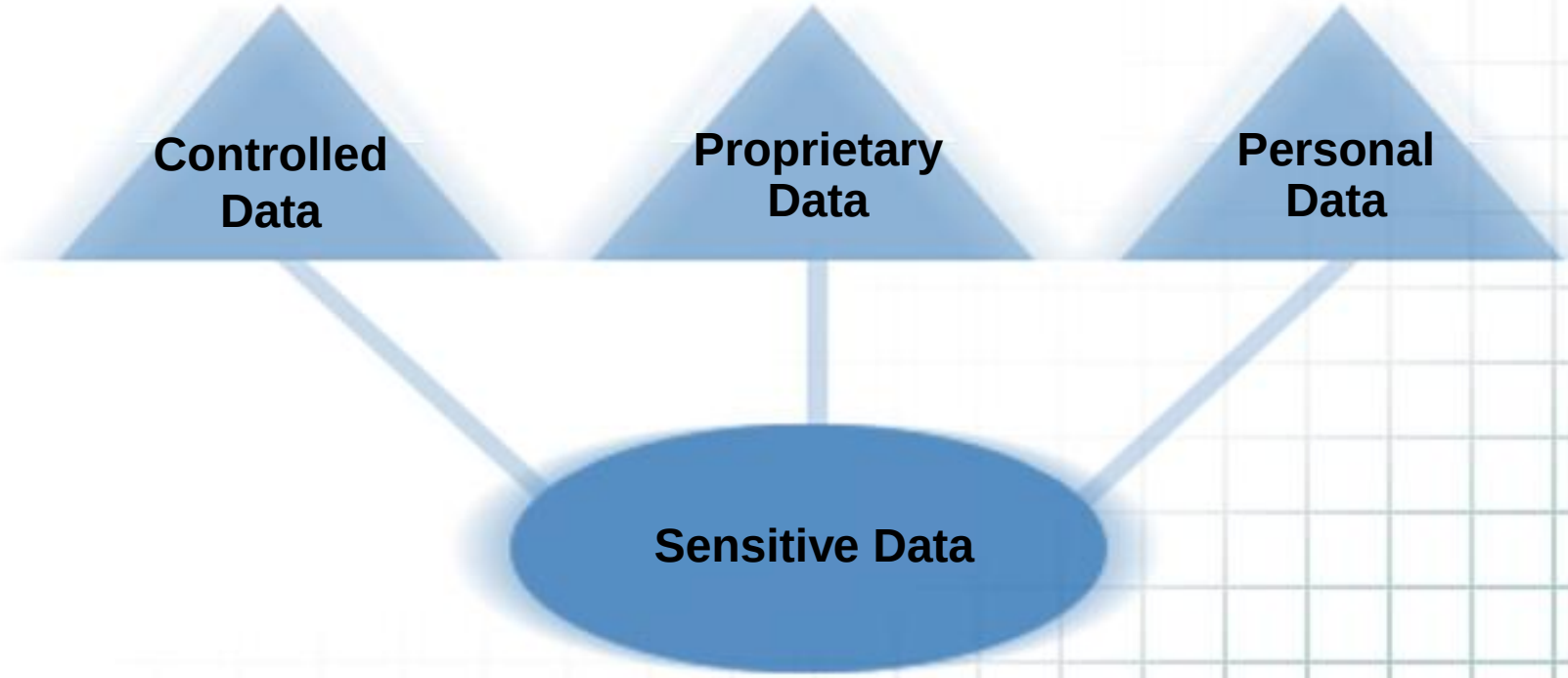
C-I-A Concerns: Access to the Data

- Confidentiality
  - No disclosure
  - Only those who need to see data should see it
- Integrity
  - No alteration
  - Only those allowed to alter data can modify it
- Availability
  - No interruption
  - Everyone who needs to access data can access it



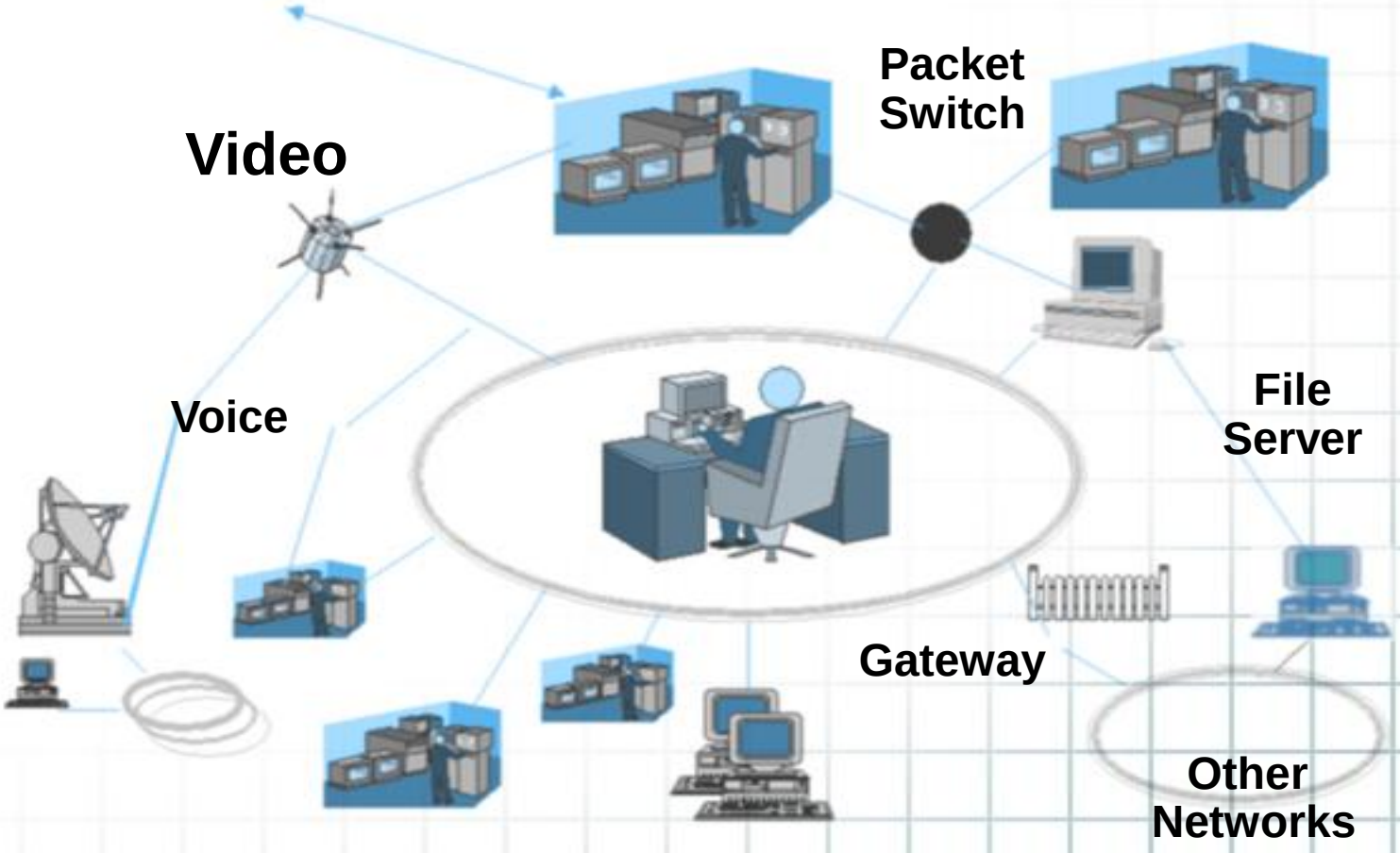
Data/Database Concerns
Data Aggregation, Data Inference & Polyinstantiation

- "The protection of the database and data elements against unauthorized access, either intentional or accidental"

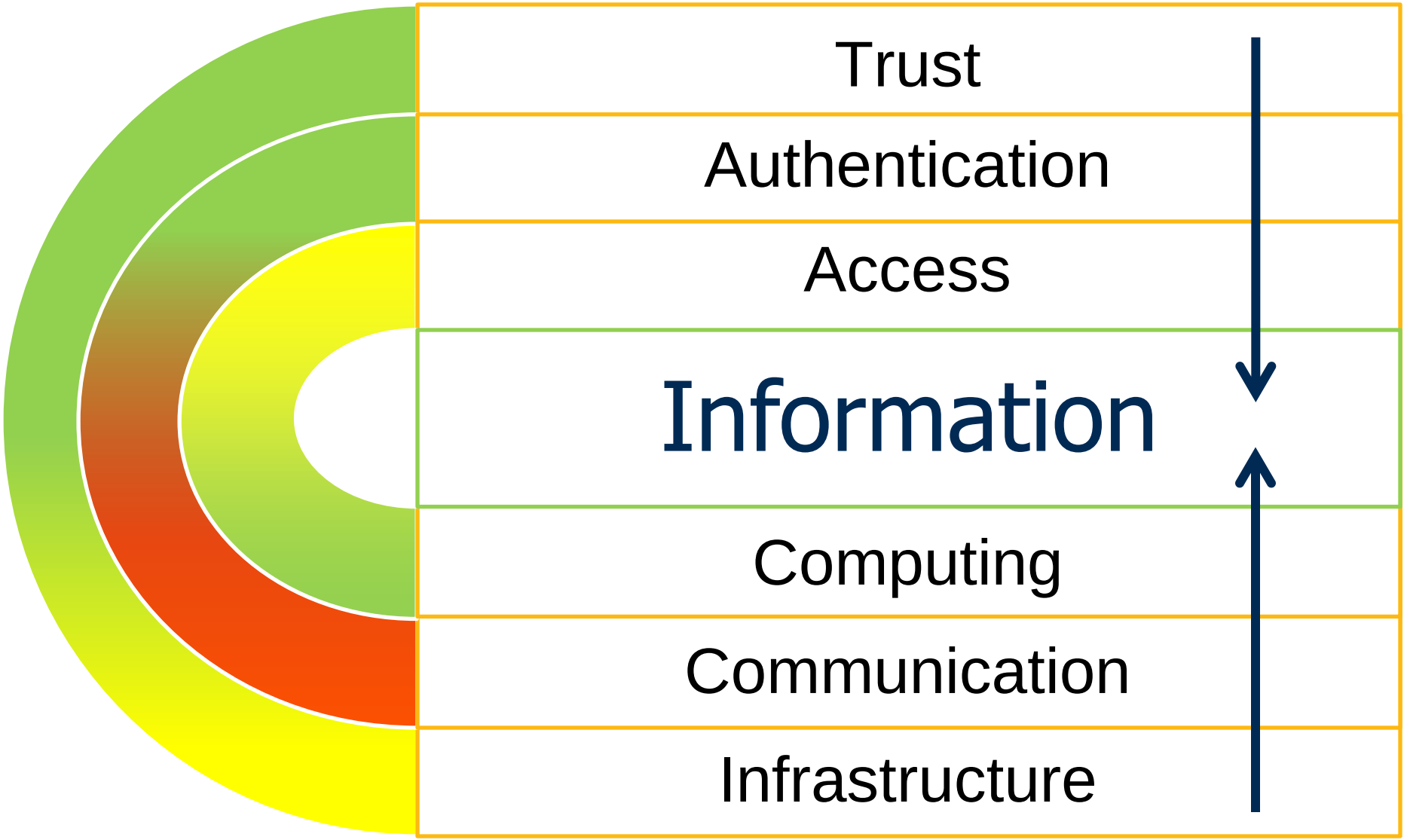


Network Concerns - Inter-Connectivity

- Hardware
- Software
- Data



IT Systems have Logical Access Layers



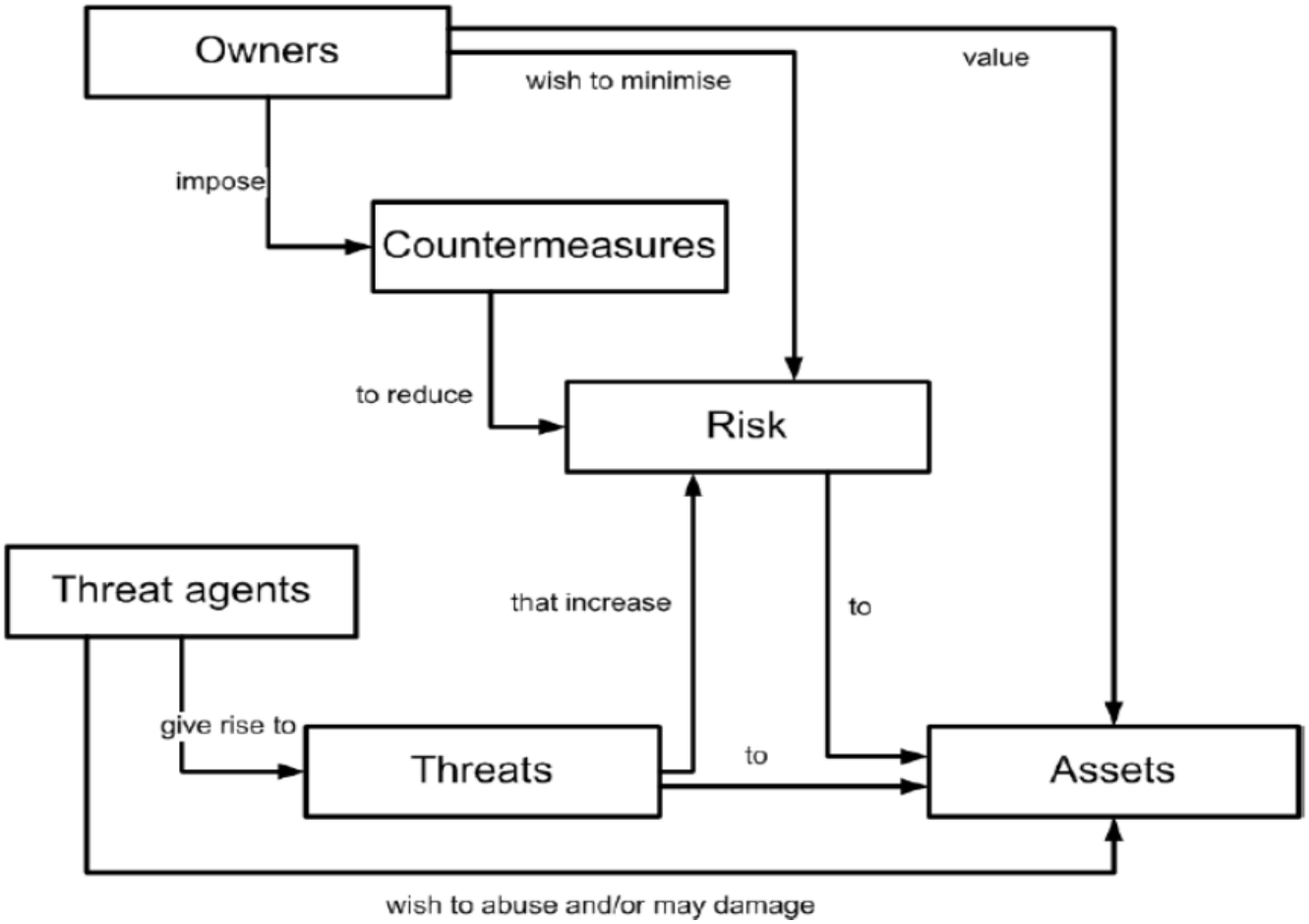
Hardware Concerns

- Access
- Theft
- Environmental considerations
- Media protection
- Media declassification/destruction
- Lack of built in security mechanisms
- Electromagnetic/Compromising Emanations
- Hardware modifications
- Hardware attacks

Software Concerns

- MALWARE, unauthorized changes to programming code, inadequate backups or backups not made, program errors.
- Copyright/intellectual property right violations.
- Low Risk - High Risk – Prohibited Software.
- Changes to the Trusted Computing Base (TCB).
- Changes to the Trusted Domain (TD).
- Software control and use.
- Freeware/Shareware/Adware/…

IA Policy Model is Risk and Threat-Based

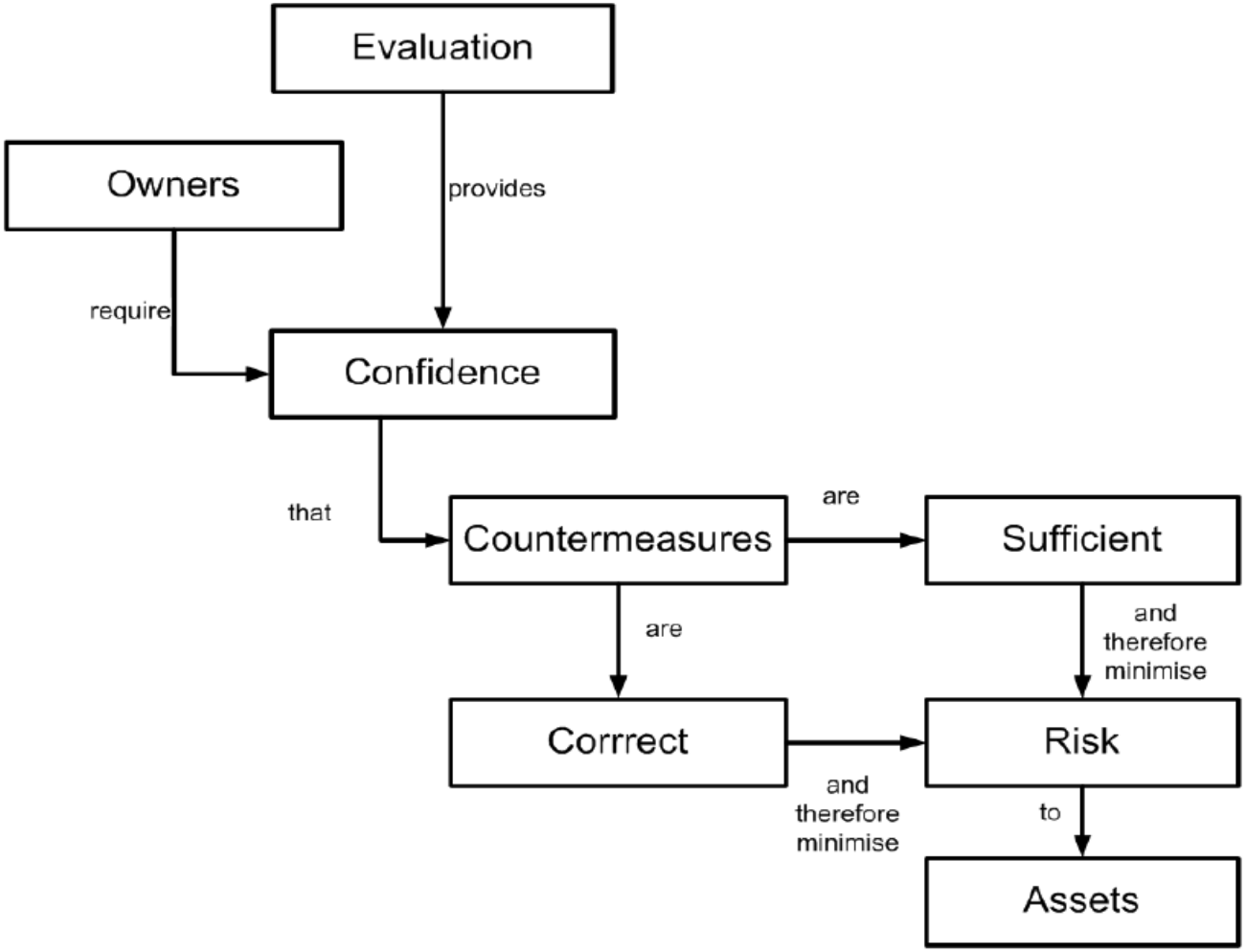


Common Criteria for Information Technology Security Evaluation
http://www.commoncriteriaportal.org/

Assets at Risk

- Hardware
  - Physical Items
  - Firmware Updates
- Software
  - Operating System
  - Application
  - Utility
- Personnel
  - Operator & System Maintainers
  - Users(Direct/Indirect)
- Data & Information
  - Collection
  - Storage
  - Stages of Process
  - Replacement Value
    - » Current Worth
    - » Short Term
    - » Long Term

IA Policy not Useful Without Evaluation



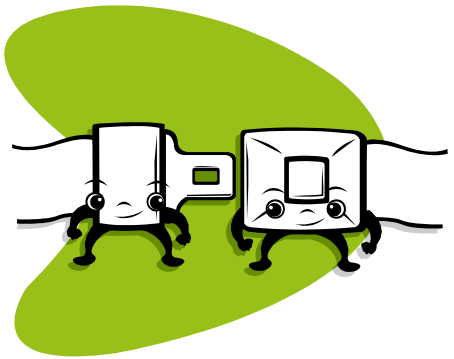
Common Criteria for Information Technology Security Evaluation
http://www.commoncriteriaportal.org/

Threat/Countermeasures (Vulnerabilities)

- People
  - Awareness/Training
  - Accountability/Incentives
  - Intent (criminal or other)
- Computing
  - Accessibility/Openness
  - Portability
  - Compactness of media
- Networks
  - Complexity
  - Accessibility/Openness
- Organizations
  - Networks/Nation States
  - Persistence & Resources
- Enterprise
  - Nature of Data
  - Lack of Built-in Security Mechanisms
  - Trust and Protection
- Software
  - Malware
  - Open App Markets

Agenda

- Introduction to Cyber Security
- Understanding the Threat
- Information Assurance
- Cyberspace as a Complex System
- Enterprise Architecture
- The System Architect
- Example Methods



Complex Systems

Georgia Institute of Technology

Complexity

the degree to which a system or component has a design or implementation that is difficult to understand and predict/verify

Complex System

a system composed of interconnected parts that as a whole exhibit one or more properties (behavior among the possible properties) not obvious from the properties of the individual parts

Sociotechnical Systems

- Social: concerning groups of people or the general public
- Technical: based on physical sciences and their application
- Sociotechnical Systems: technical works involving significant social participation, interests, and concerns
  - The architecture and design of these systems is affected by the participation of groups of people

Because of the influence of technology, almost every system today is a sociotechnical system

Systems of Systems

- Key considerations in architecting systems of systems, with respect to sociotechnical elements
  - Autonomy or Operational Independence: the user can define their interaction with parts of the system
  - Emergence: the system will evolve over time
  - Connectivity or Net-centricity: information about the system is available to all as needed
  - Managerial control: the overall behavior of the system can be influenced by the architect

Maier
Operational independence
Managerial independence
Evolutionary development
Emergent behavior
Geographic distribution

Boardman/Sauser
Autonomy (of individual systems)
Belonging (of individual systems)
Connectivity
Diversity
Emergence

Complex Systems

- Are **non-linear and dynamic** and do not inherently reach fixed equilibrium.
- Are composed of **independent agents** whose behavior is not necessarily driven by the system dynamics.
- Because agents needs or desires are not homogeneous, their **goals and behaviors are likely to conflict**.
- There is **no single point of control**. Behaviors are easier to influence than to control.
- Behavior of complex systems is **temporal**, and is often unpredictable beyond near-term states.
  - Short-term changes can produce chaotic behavior
  - Long-term performance is characterized by feedback in the system

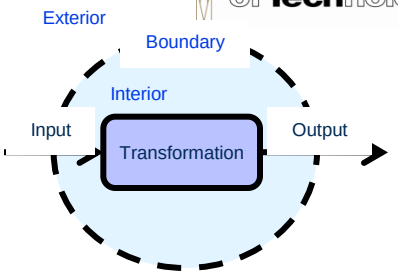
Rouse: Healthcare as a Complex Adaptive System: Implications for Design and Management

Complex Adaptive Systems

- Are characterized by **intelligent agents**. Agents learn and change their behavior over time, and the system's behavior changes over time.
- Adaptation and learning tend to result in **self-organization**. Behavioral patterns tend to emerge rather than be designed.
- One cannot command or force the system to comply with behavioral and performance dictates using conventional means.
- One cannot analyze the performance of such systems using conventional systems engineering disciplines centered around hierarchical decomposition.

Rouse: Healthcare as a Complex Adaptive System: Implications for Design and Management

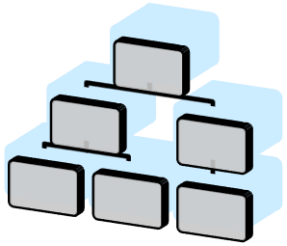
Understanding & Synthesizing Complex Systems



Boundaries

- Scope: Boundary, Interior, and Exterior

Inter-relationships



- Function: Inputs, Outputs, Transformations
- Structure: Hierarchy, Openness, Emergence
- Governance: Command, Control, Communication

Perspective

- Process: Wholes, Parts, Relationships
- Vision: Variety, Economy, Harmony

Adapted from Boardman, J. T. and B. J. Sauser (2008). Systems Thinking: Coping with 21st Century Problems. Boca Raton, Taylor & Francis.

Designing Complex Systems

- Complex sociotechnical systems should be designed and should not just emerge
- Complexity can be managed by providing structure, and a design focused on managing the complexity
  - Rules of order
  - Rules of simplification
- The complex system is managed by monitoring and influencing systems state, system performance, and stakeholder behavior
- Keys are information and incentives

Comparing Organizational Behaviors

	Traditional System	Complex System
Roles	Management	Leadership
Methods	Command and Control	Incentives and Inhibitions
Measurement	Activities	Outcomes
Focus	Efficiency	Agility
Relationships	Contractual	Personal Commitments
Network	Hierarchy	Heterarchy
Design	Structured	Self-organizing

- Interrelationships drive the need for governance processes as part of the system design
- System performance measured in outcomes and values, not necessarily on a defined timescale

Rouse: Healthcare as a Complex Adaptive System: Implications for Design and Management

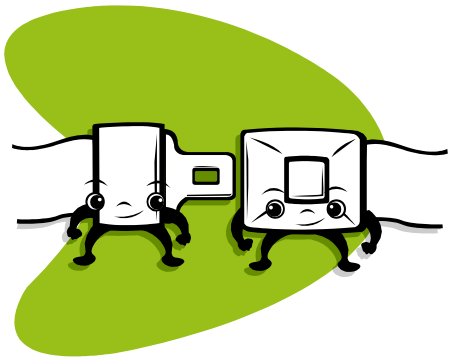
Perspective in a Complex System

- Viewing the system in a holistic manner (as a whole) leads to better decision making
- Openness of information will improve performance
- Behaviors will be driven by the value of outcomes from system functions
- Self-organization around vision and goals defined around valued outcomes will help the system change and improve
- Incentives are necessary to drive preferred outcomes

Rouse: Healthcare as a Complex Adaptive System: Implications for Design and Management

Agenda

- Introduction to Cyber Security
- Understanding the Threat
- Cyberspace as a Complex System
- Information Assurance
- Enterprise Architecture
- The System Architect
- Example Methods



Systems “Architecting” vs. “Engineering”

Georgia Institute of Technology

- Systems architecting differs from systems engineering in that it relies more on **heuristic** reasoning and less on use of analytics

- There are **qualitatively** different problem solving techniques required by high and low complexity levels
  - The lower levels would certainly benefit from purely analytical techniques, but those same techniques may be overwhelming at higher levels which may benefit more from heuristics derived from experience, or even abstraction
  - It is important to concentrate on only what is essential to solve the problem

The system should be modeled at as a high a level as possible, then the level of abstraction should be reduced progressively as needed

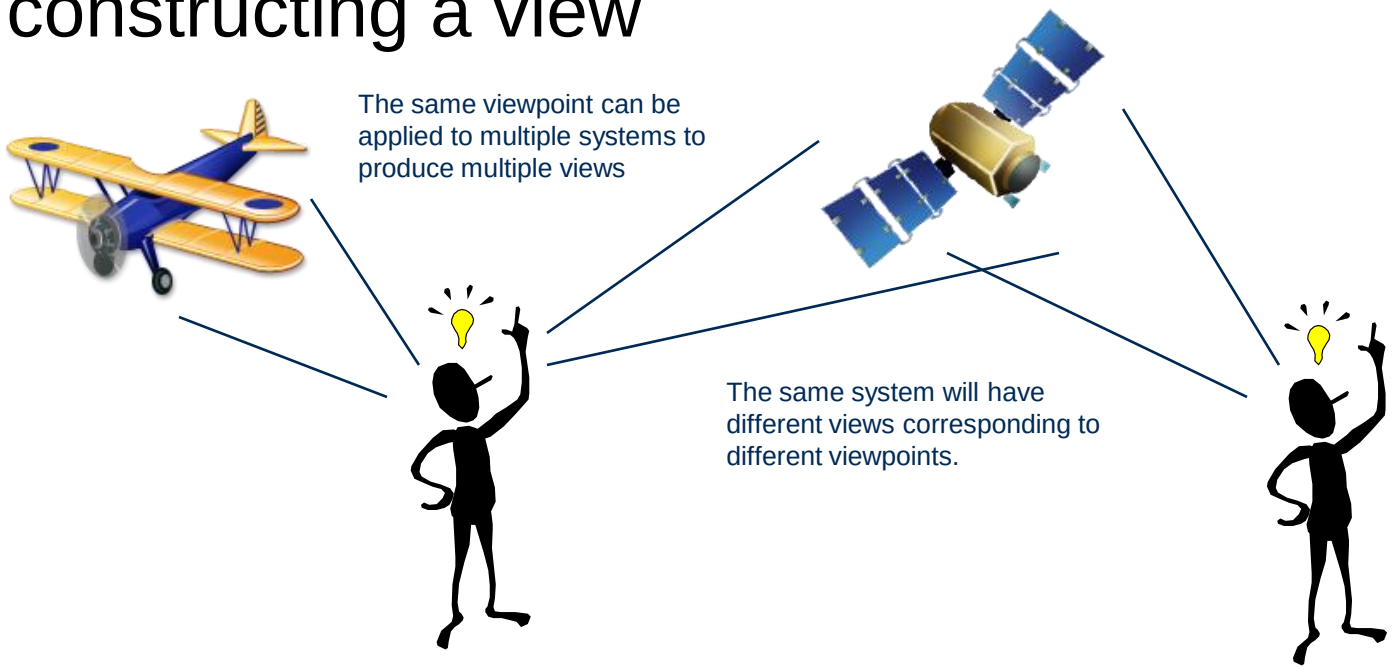
Normative Requirements for Architecture Description

- The stakeholders identified must include users, acquirers, developers, and maintainers of the system
- The architectural description must define its viewpoints, with some specific elements required
- The system's architecture must be documented in a set of views in one-to-one correspondence with the selected viewpoints, and each view must be conformant to the requirements of its associated viewpoint
- The architecture description document must include any known interview inconsistencies and a rationale for the selection of the described architecture

source: IEEE-1471-2000 ; Maier (2009)

Views and Viewpoints

- A **View** is a representation of a system from the perspective of related concerns or issues
- A **Viewpoint** is a template, pattern, or specification for constructing a view



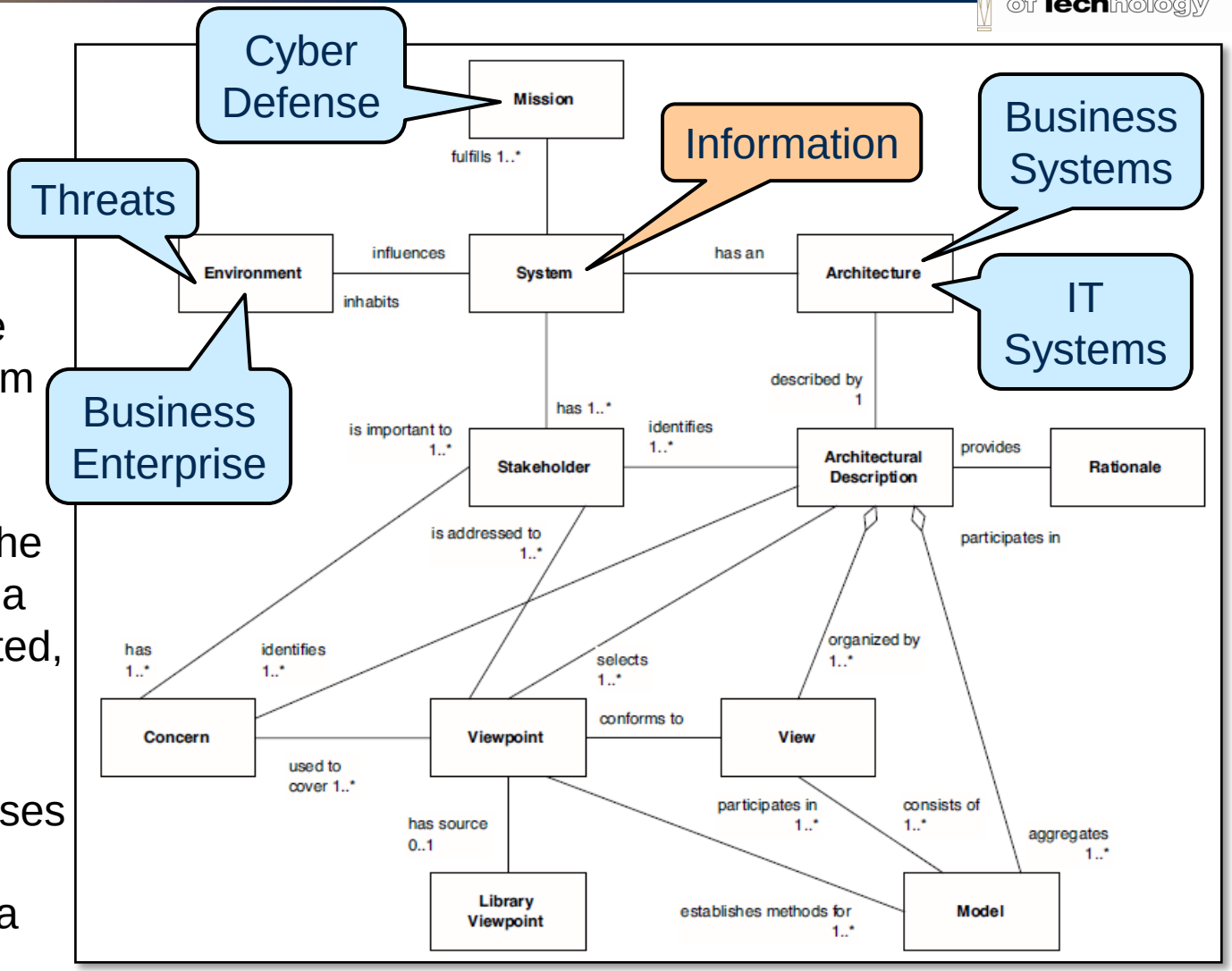
terms: IEEE-1471-2000
Graphics adapted from: Maier (2009)

Enterprise View ⇔ Viewpoint Examples

- Organization ⇔ Org Chart
- Business Policy ⇔ Employee Handbook
- Business Policy ⇔ Policies & Procedures Manual
- Business Policy ⇔ IT Workflow Design
- IT Architecture ⇔ High Level Graphic (OV-1)
- IT Architecture ⇔ Subsystem Description (SV-1)
- IT Architecture ⇔ Bill of Materials
- Business Event ⇔ Invoice
- Business Event ⇔ Disaster Scenario

IEEE-1471-2000:
Conceptual Model of an Architectural Description

- Includes stakeholders and their concerns as fundamental element
- The environment determines the boundaries that define the scope of the system of interest relative to other systems
- Viewpoints establish the conventions by which a view is created, depicted, and analyzed
- Views conforms to a viewpoint, and addresses concern(s) of the stakeholders through a model



Graphics: IEEE-1471-2000

Enterprise Architecture

- A building plan for a system or system of systems
- Documentation of the enterprise model set that comprise the people, processes, policies, and information required to design and manage the business
- Documentation of the high-level design decisions made by the architects of the business systems, capturing Heuristic and Narrative descriptions
- Documentation of the lower level design decisions made by the developers of the business systems, capturing requirements, models, structure, function

Enterprise Architecture Frameworks

Provide high level models for the development, documentation, and management of enterprises

- DoD Architecture Framework (DODAF)
  - Architectural Model for View ⇔ Viewpoint Capture
- Zachman Framework for Enterprise Architecture
  - Enterprise Model for View ⇔ Viewpoint Capture
- The Open Group Architecture Framework (TOGAF)
  - Enterprise Architecture process model
- Systems Modeling Language (SysML)
  - Model-Based Systems Engineering tools for all the above
- And others…

The Zachman Framework for Enterprise Architecture™

The Enterprise Ontology™

Version 3.0

Use of the Zachman Framework here

	What	Who	Why	Where	When	How
Executive		*Planners*		System	Views	
Business Process		*Owners*				
System		*Designers*				
Developer		*Builders*				
Operator		*Toolsets*				
Enterprise		*Users*				
	Business Aspirations: Values, Goals, etc.					

Perspective Views

Work Product Generation Principles

	What	Who	Why	Where	When	How
Executive						
Business Process						
System						
Developer						
Operator						
Enterprise						

- The Zachman Framework defines primitive elements
  - Each cell then presents an example of a single-variable model
  - The columns present more detail
  - The relationship of the rows is not defined
- Composite models are defined by row primitives
  - The composite model create the work products
  - Used them to define the view bridged models

Enterprise Framework Perspectives

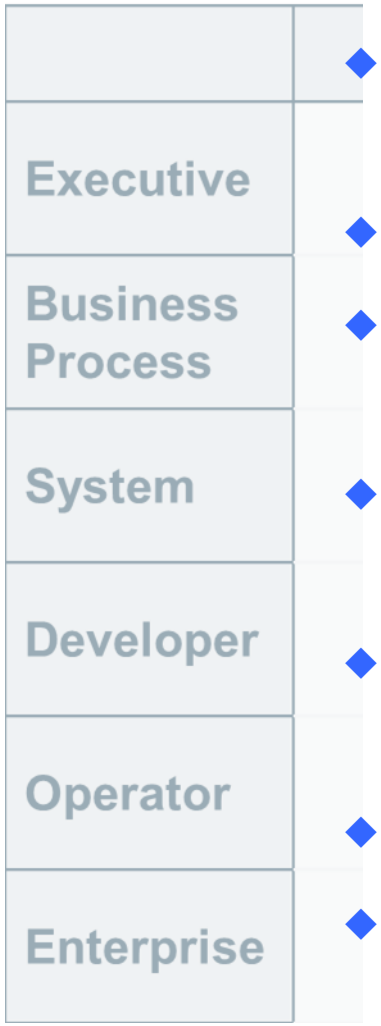
	What	Who	Why	Where	When	How
Executive						
Business Process						
System						
Developer						
Operator						
Enterprise						

- **Abstract**: valuation (IP, strategy,…)
- **Relational**: links between people and systems/ processes/events, formal and informal roles
- **Virtual**: intangible artifacts (data, software,…), virtual locations, process implementation, virtual events, people skills
- **Physical**: tangible artifacts (computers, buildings,…), mechanical processes, physical events, physical work
- **Aspirational**: reason for being (vision, values, principles…)

Business Asp

Tom Graves, Bridging the Silos: Enterprise Architecture for the IT Architect, Tetradian Books, December 2008

Enterprise Framework Layers



- **Universal**: in principle things that wouldn't change or change infrequently: vision, values, etc.
- **Executive**: long-term change: strategy
- **Business**: organization, relationships, dependencies, measures
- **System**: architecture: abstracting from the logical form to the implementation forms
- **Developer**: real-world design attributes: systems and processes, policies and training
- **Operator**: devices, tools, deployment, instruction
- **Enterprise**: actual users and use cases

Enterprise Framework Primitives

- Assets – ***what?***
  - Abstract: financial, HR, Intellectual Property
    - » Models: financial, business process,…
  - Relational: links to people- employees, customers
    - » Models: identities, roles, access,…
  - Virtual: data, metadata, messages…
    - » Models: data model, schemas,…
  - Physical: servers, routers, paper,…
    - » Models: networks, bill-of-materials,…
  - Aspirational: vision, values, strategy…
    - » Models: strategic plans

	What	Who
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		

Enterprise Framework Primitives

- Capabilities – ***who?***
- People (actors, agents) – capabilities are clustered into *roles*
- Roles are abstract, characterized by skills and training, within business processes, include:
  - Abstract – Principle-based: leadership, values, culture
  - Relational - Heuristic: recognizing cause-effect and patterns
  - Virtual - Analytic: based on experience, judgment…
  - Physical - Rule-based: choice not permitted
    - » Could be implemented by people or machines

	Who	Why
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		

Enterprise Framework Primitives

- **Reasons** – ***why?***
- Generally defined as *decisions*
- Business rules, requirements, constraints, strategy, tactics - include:
  - Abstract – Principle-based: guiding principles
  - Relational - Heuristic: context, trust, risk
  - Virtual - Analytic: best practices, links *who, what, how*
  - Physical - Rule-based: laws, mandates, regulations, policies

	Why	Where
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		

Enterprise Framework Primitives

- Locations – ***where?***
  - Abstract: temporal locations
    - » Models: project schedules, timelines,…
    - » Note that time is "*where*" not "*when*"
  - Relational: people locations, organizational structure
    - » Models: directories, org charts, social network maps,…
  - Virtual: network IDs, IP addresses, phone numbers…
    - » Models: network maps, file structures,…
  - Physical: buildings, rooms, clouds,…
    - » Models: maps, schematics,…

	Where	When
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		

Enterprise Framework Primitives

- Events – ***when?***
  - Abstract: business cycles
  - Relational: people – meetings, action items,…
  - Virtual: messages, data triggers,…
  - Physical: normal (monthly/weekly), abnormal (incidents, disasters),…

	When	How
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		

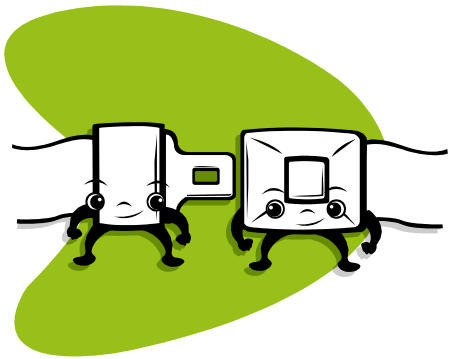
- Functions – ***how?***
  - Abstract: how business processes are performed
  - Relational: links to people- employees, customers
  - Virtual: data transformation or other virtual information
  - Physical: transformation of physical objects,…

Use of the Zachman Framework Here

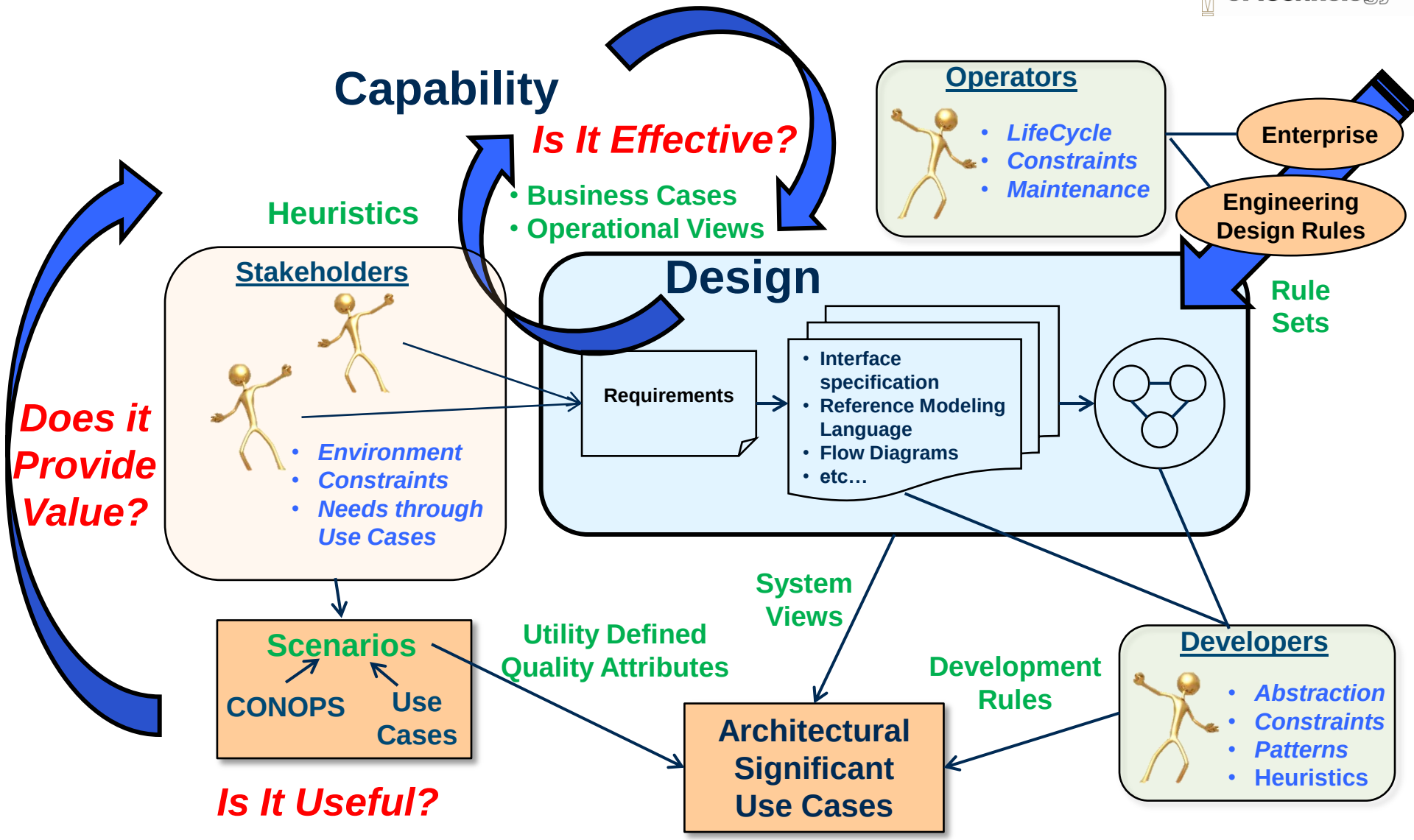
	What	Who	Why	Where	When	How
Executive	Abstract: IP, etc.	Values, Virtues	Principles	Time	Business Cycle	
Business Process	Relational	Relation-ships	Policy	Organiza-tional	Normal, Abnormal	Relational
System	Virtual	Manage-ment	Context	Opera-tional	Process	Conops, Use Case
Developer	Virtual, Physical	Policy, Process	Use Cases	Structural	Commun-ication	Interface
Operator	Physical	Rules	Needs	Physical	Triggers	Instruc-tion
Enterprise	Information !!!	Roles	Regulatory Legal	Access	Business Cycle	Work
	Business Aspirations: Values, Goals, etc.					

Agenda

- Introduction to Cyber Security
- Understanding the Threat
- Cyberspace as a Complex System
- Information Assurance
- Enterprise Architecture
- The System Architect
- Example Methods



Perspective of the Systems Architect



Phases of Architecting

Georgia Institute of Technology

Changes as project moves from phase to phase

Early	**Mid**	**Completion**
Structuring of the unstructured (need, solutions, technical possibilities)	Integration of competing (sub)systems and interests	Certification that systems is suitable for use
Art	*Rational and Normative*	*Art and Science*
Narrative Form	Specific Form	Narrative and Measured Forms

Language of the Architect

Georgia Institute of Technology

Changes as project moves from phase to phase

Early	Mid	Completion
• Heuristics • Stories • Con-ops • Scenarios *Art*	• Requirements • Behavior • Structure • Function • Rules *Rational and Normative*	• Performance • Analysis • Evaluation • Utility *Art and Science*
Narrative Form	Specific Form	Narrative and Measured Forms

The Role of the System Architect

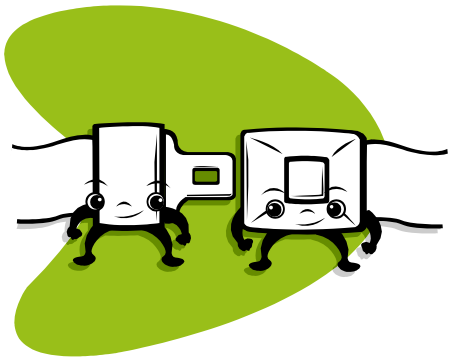
- The System Architect is more a leadership and management role than a technical role
- Architects need experience, and a blend of management and leadership disciplines
- Communication and vision require leadership capacity
  - The architect holds the architectural vision, often their own
  - The architect makes high-level design decisions around interfaces, functional partitioning, and interactions
  - The architect must communicate these effectively, often visually
- The architect's primary tasks are rule-setting
  - The architect must direct technical standards, including design standards, tools, or platforms,
  - These should be based on business goals rather than to place arbitrary restrictions on the choices of developers and operators.

The Role of the System Architect

- The System Architect uses interviews to collect concepts, use cases, and stakeholder perspective
- The System Architect facilitates brainstorming techniques to arrive at commonly accepted con-ops and use cases
  - Scenarios are collected and used to reach agreement
  - Architecturally significant scenarios are collected and saved for evauation
- The System Architect uses visual methods and stories to articulate the specific forms
- The System Architect uses evaluative techniques to determine architectural attributes of the design
- Model, model, model,…

Agenda

- Introduction to Cyber Security
- Understanding the Threat
- Cyberspace as a Complex System
- Information Assurance
- Enterprise Architecture
- The System Architect
- Example Methods



TOGAF Architecture Development Cycle

A. Vision, values, strategy, etc

B. Business drivers

C1. Information Architecture

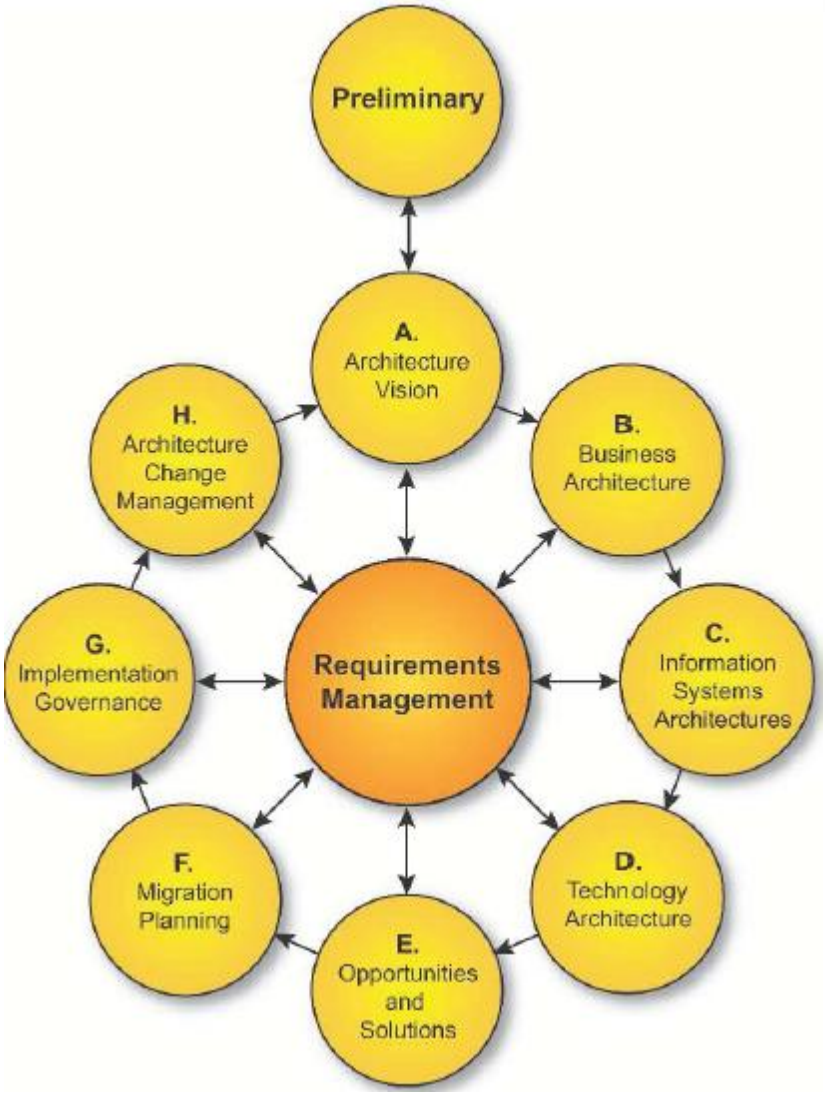
C2. Information Systems

D. Development Process

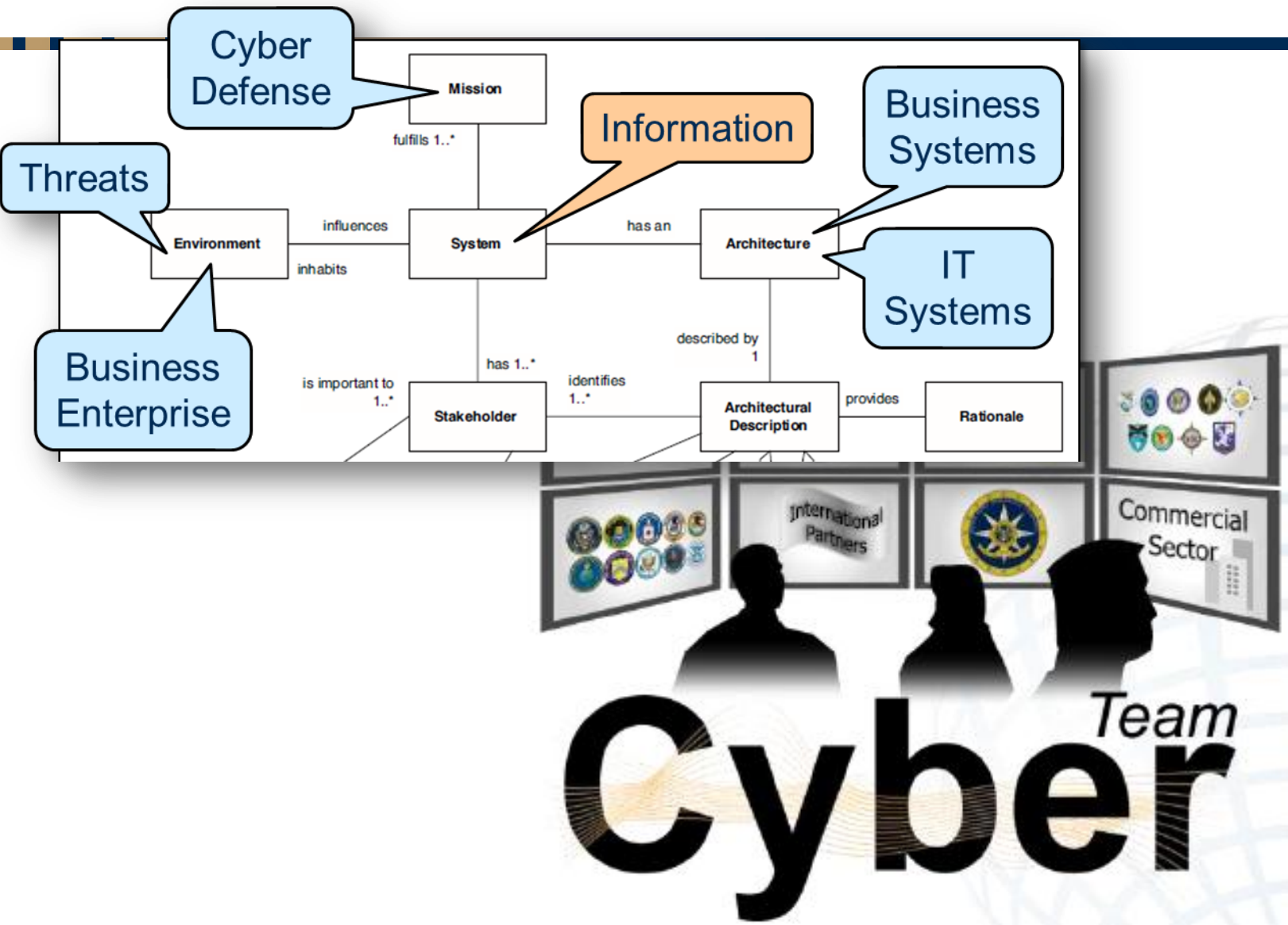
E. Deployment Process

F, G. Change Management

H. Configuration Management

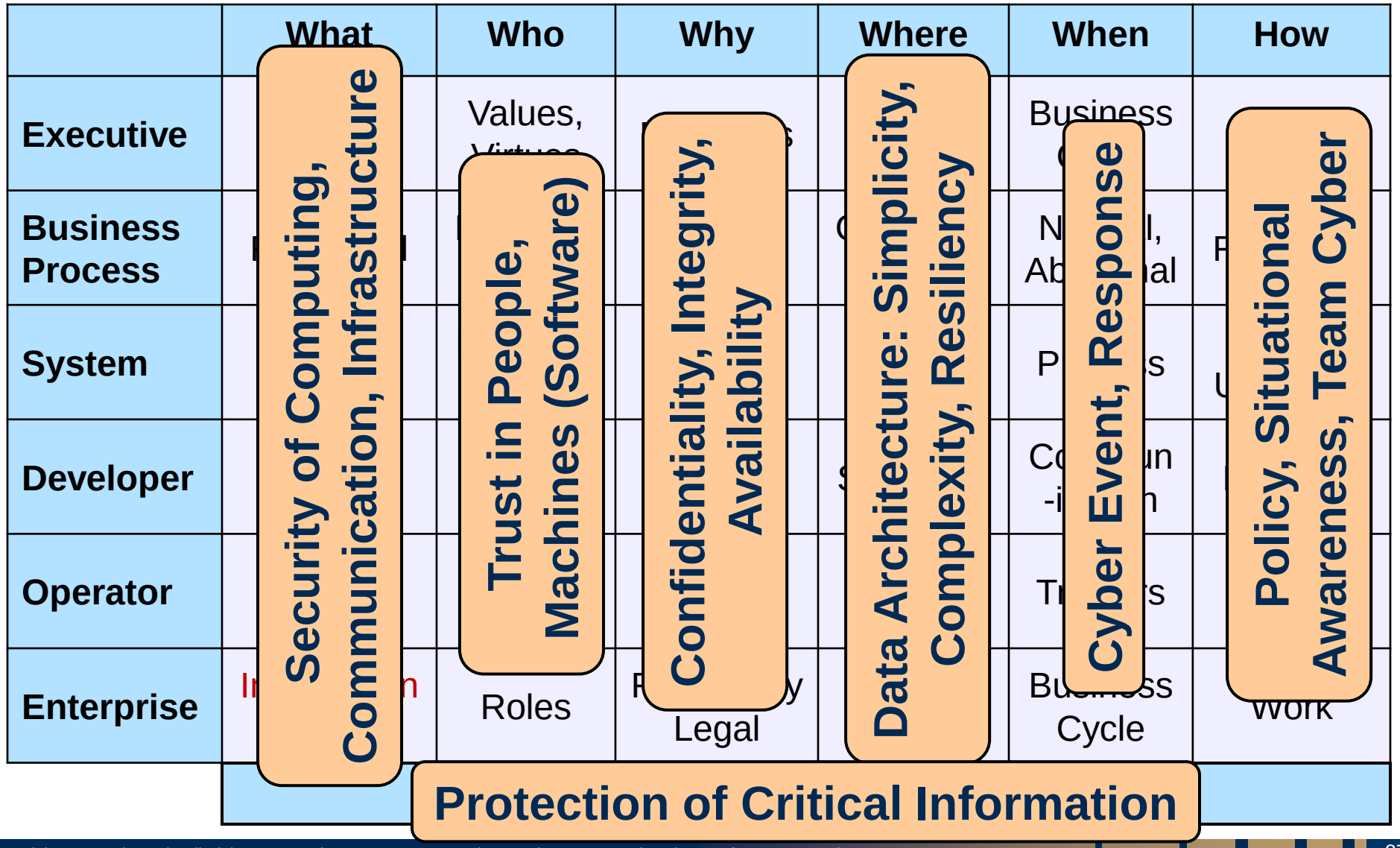


Vision and Strategy

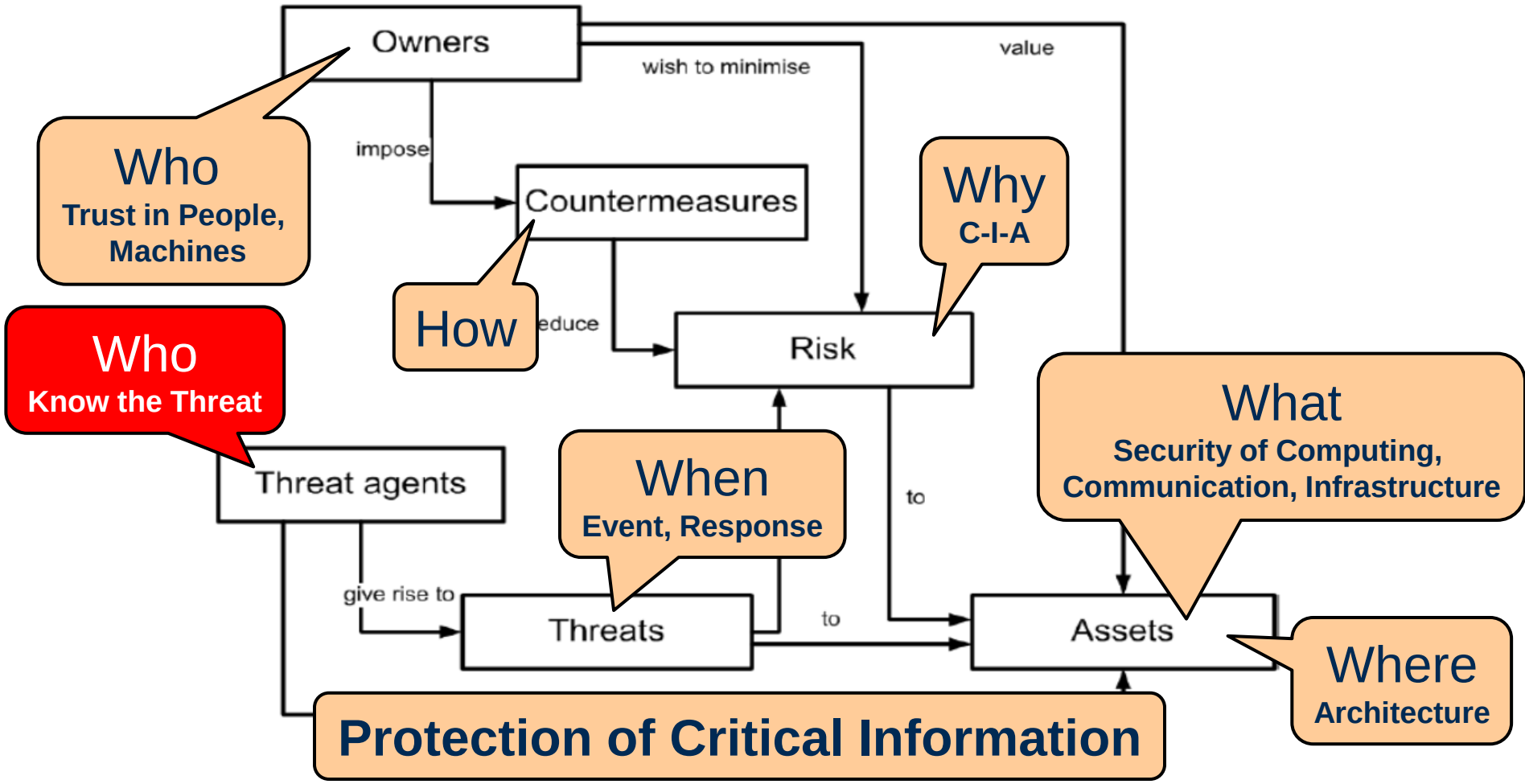


2010 US Cyber Command Briefing

Business Drivers for Cyber Defense



Enterprise Relationships for Cyber Defense



Common Criteria for Information Technology Security Evaluation
http://www.commoncriteriaportal.org/

Return to the Beginning

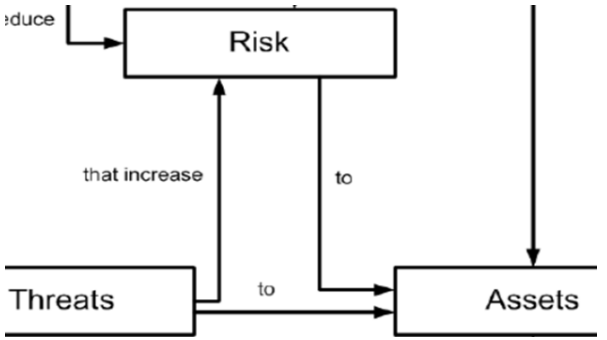
1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?
   - » Understanding your threats and threat level

Business Drivers: Starts with the Information

- What? – are the data items to protect
- Who? – is trusted to have access
- Why? – do they need to know
- Where? – does it live and get accessed from
- When? – is it used
  - Properly & Improperly
- How? – is it assigned and accessed
  - Awareness & Response

Views & Viewpoints: Information Policy

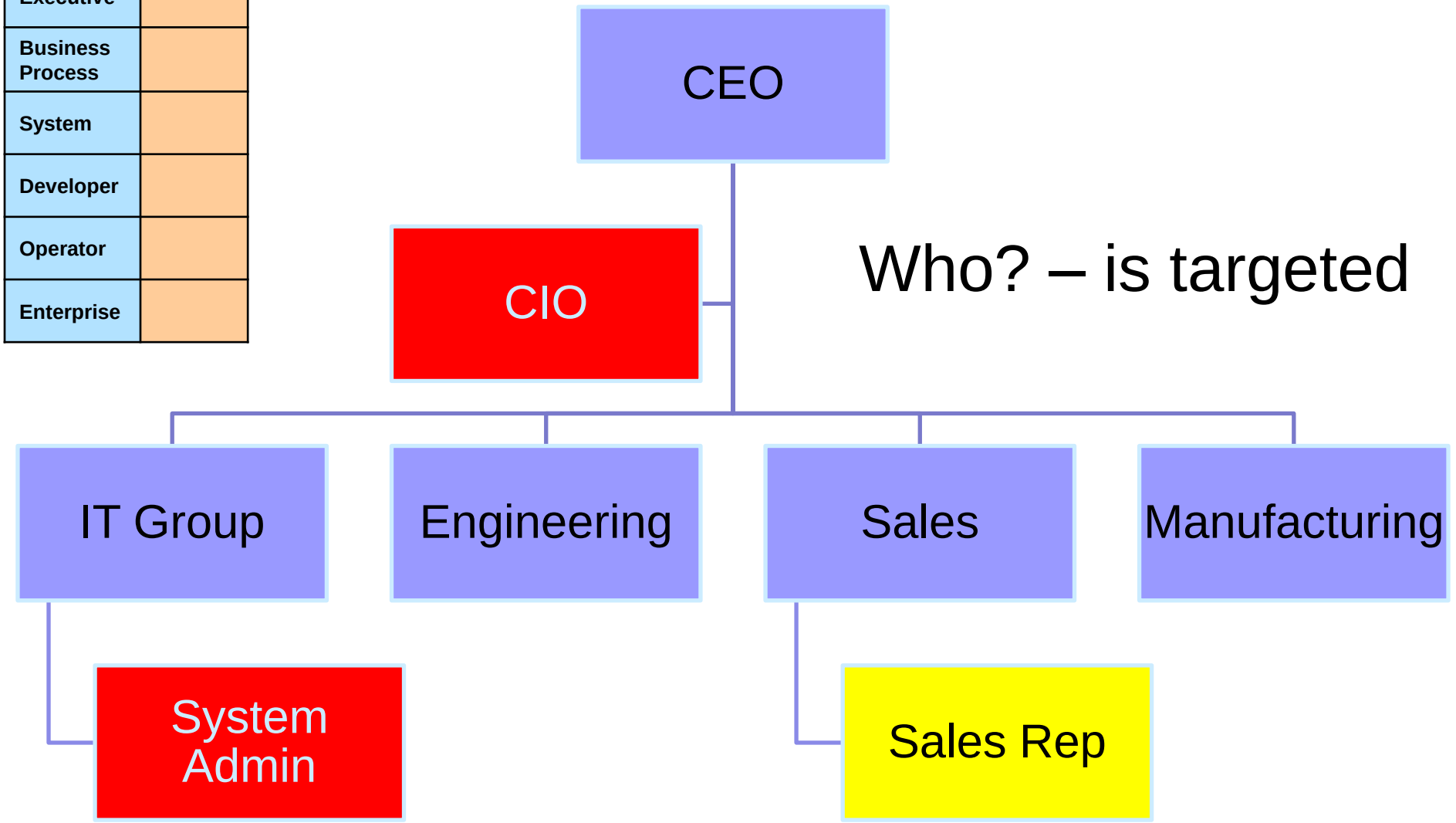
- People Views: Have an Information Asset Protection Policy
  - Employee Confidentiality Agreements
  - External Third-Party Agreements
  - Employee Policy
  - Entrance & Exit Interviews
- Information Views: Define and Document
  - Information Audit Process
  - Defined Information Access Levels
  - Marking and Labeling



	What	Who
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		

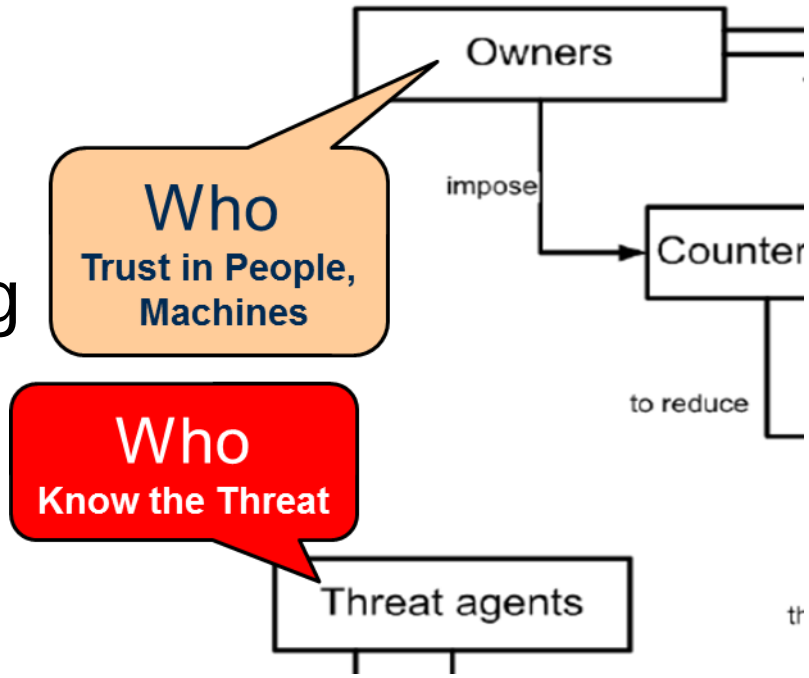
Who? – is trusted to have access

	Who
Executive	
Business Process	
System	
Developer	
Operator	
Enterprise	



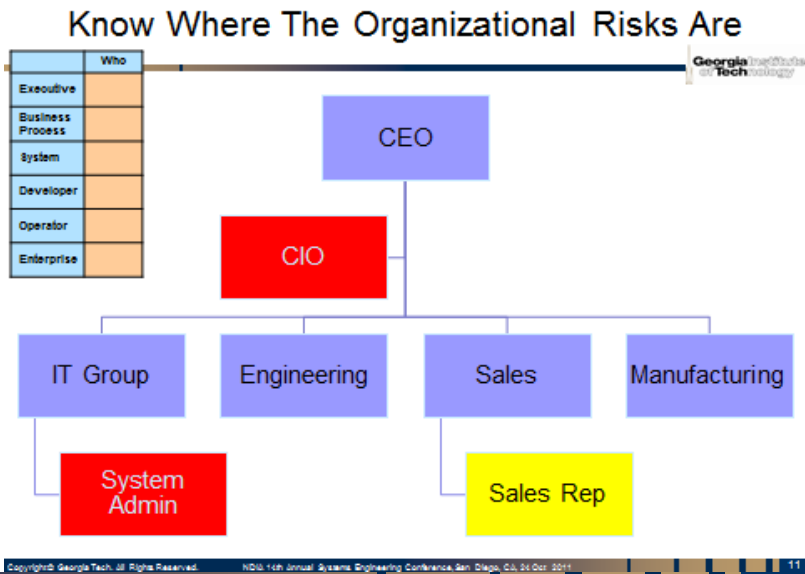
The Insider Threat

- Scenario 1: The disgruntled employee gains access to and leaves the company with valuable IP
- Scenario 2: the well placed cyber thief gains access to controlled information via personal access to IT administrators
- Scenario 3: a professional cyber thief targets various employees with a spearfishing email in an attempt to plant a virus that will monitor for administrator passwords



Scenario 1: Malicious Employee

- Many insiders who steal IP do so within 30 days prior to their termination
- Countermeasure: The primary vehicle for data exfiltration over the network is corporate email systems or web-based personal email
  - ***if*** *the mail is from the departing insider*
  - ***and*** *the message was sent in the last 30 days*
  - ***and*** *the recipient is not in the organization's domain*
  - ***and*** *the total bytes summed by day are more than a specified threshold*
  - ***then*** *send an alert to the security operator*



Source: Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination, TECHNICAL NOTE CMU/SEI-2011-TN-024, Copyright 2011 Carnegie Mellon University

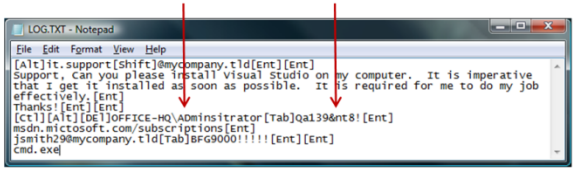
Scenario 2: Social Engineering

- Gaining internal access to IT “keys”
- Malicious Insider + Unsuspecting IT Admin
- Countermeasures:
  - Admin privileges and training
  - Scanning and Pen Testing
  - Distributed directory access

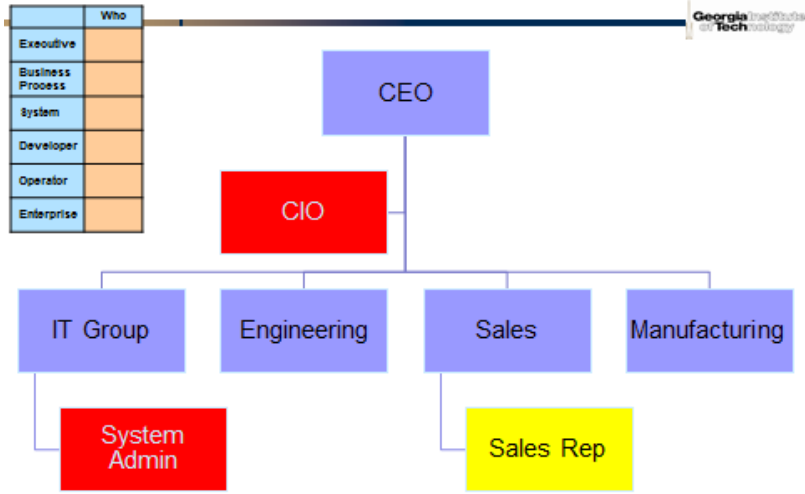
- Start Simple: Use a hardware based keylogger
  - Provided physical access

- Install Keylogger
- Call IT for help – Have something fixed/installed
- Collect their credentials
- Enjoy!

Username / Password

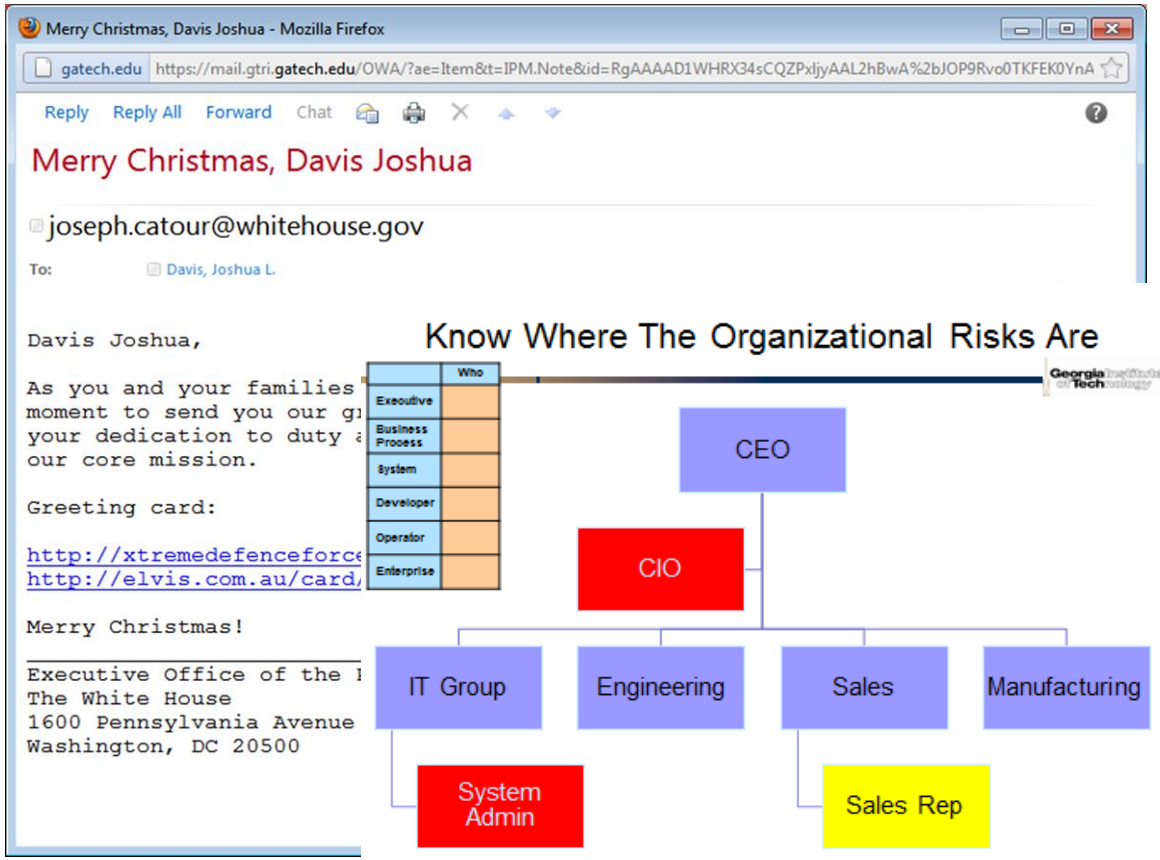


Know Where The Organizational Risks Are



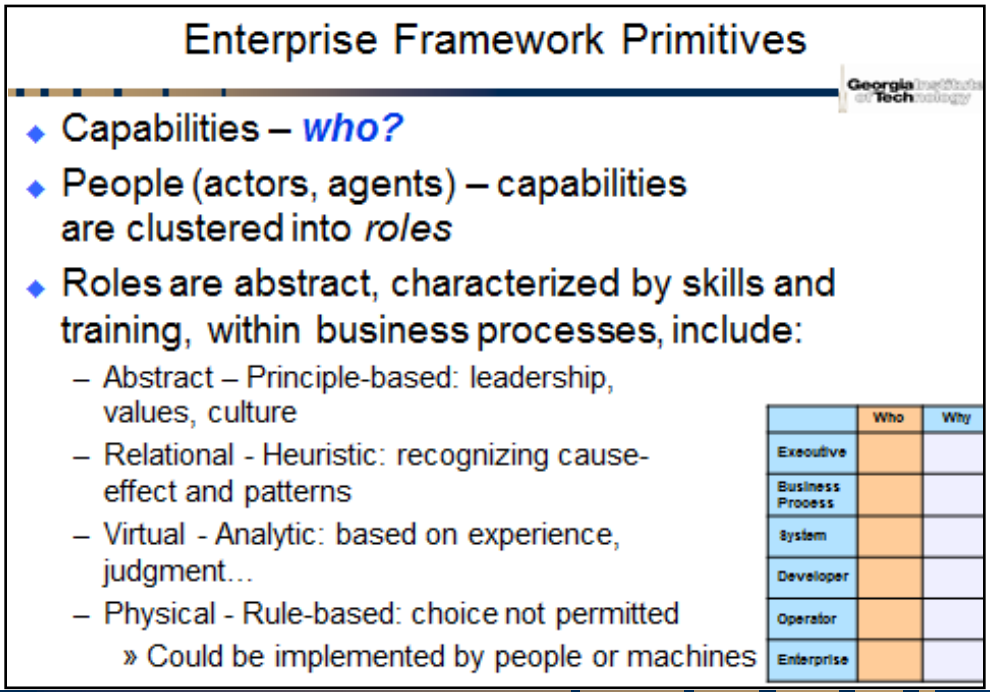
Scenario 3: Phishing

- Phishing is a way of attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.
- The web link brings a drive-by attack
- Countermeasures:
  - Awareness
  - Scanning
  - Pen Testing
  - Malware Tools



Identity Architecture: A "System" Horizontal

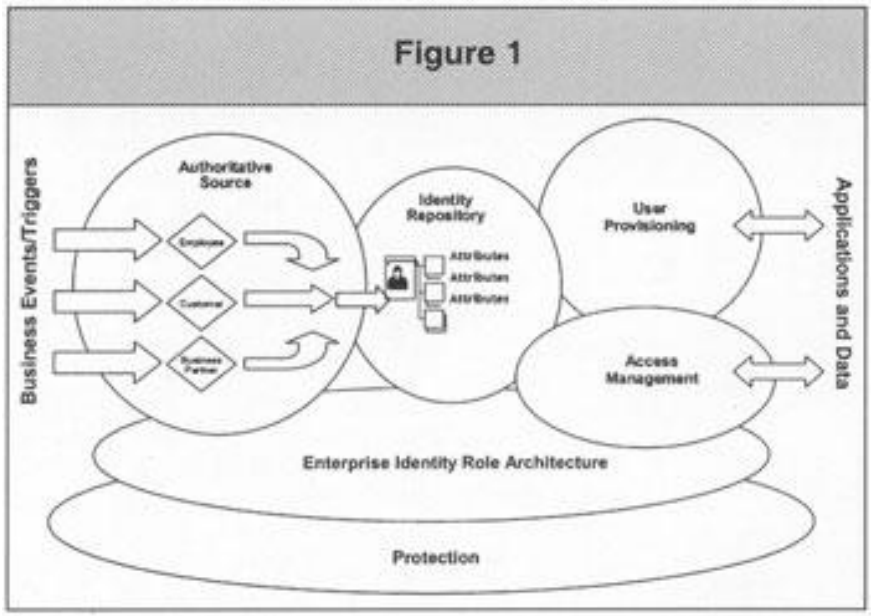
- Connects the Physical Person to the Virtual Cyber-Persona to the Logical Information Systems Network to physical Information locations
- Includes processes and methods that enables individuals to identify themselves to information systems in a consistent and coherent manner
- Ideally enables identification once and authorization many times
- Has the ability to add or delete authorizations



1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?

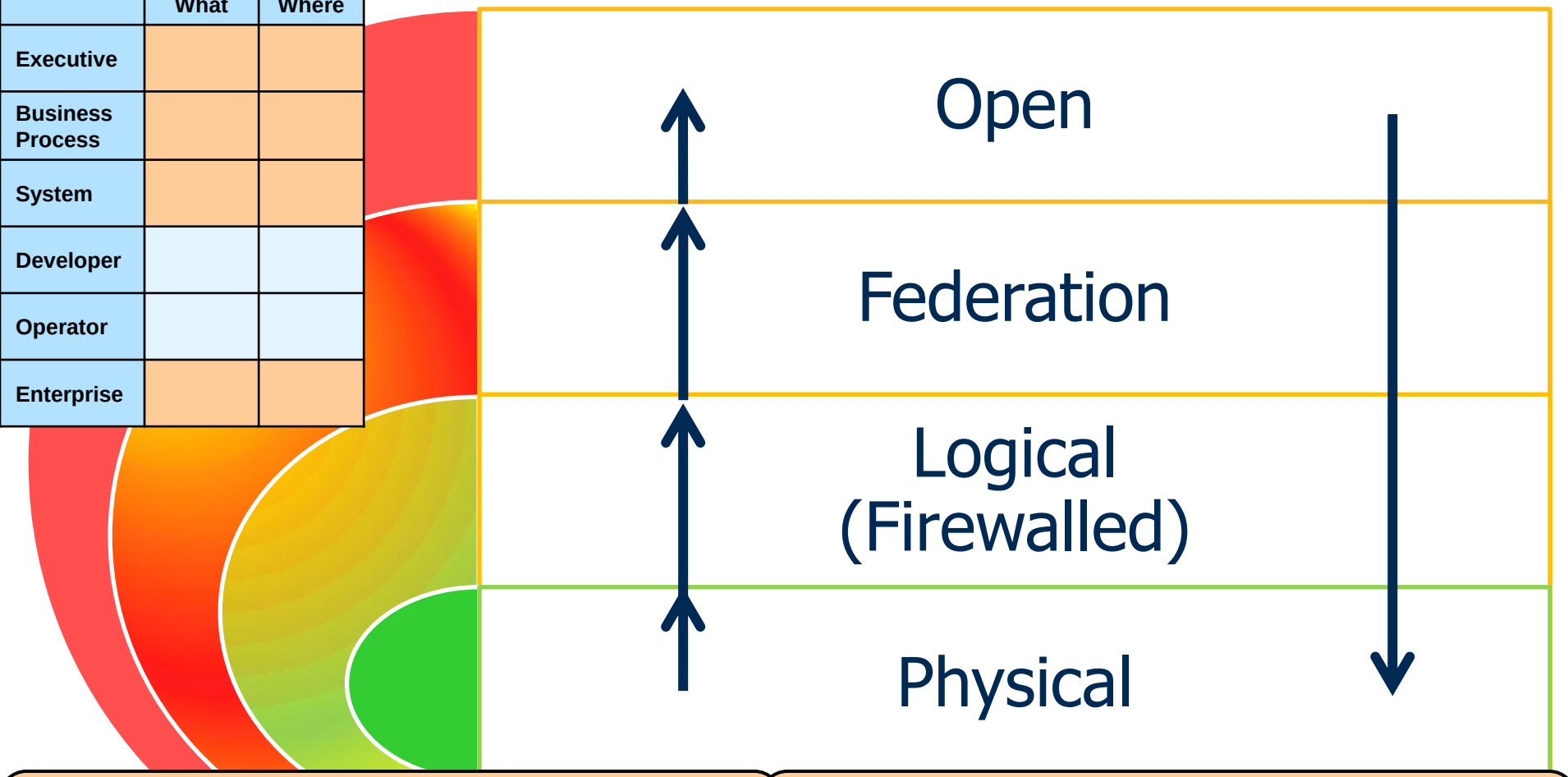
Identity Architecture

- Business Events (*When*)
  - Hiring an employee, establishing a team, federation, …
- Authoritative Source (*Who, What*)
  - Database of authorized identities and access
- Identity Repository (*Where*)
  - Ties authority to IT, Ex. Lightweight Directory Access Protocol (LDAP)
- User Provisioning (*Where, Why*)
  - Provisioning the IT applications with identities and access authority
- Access management (*How*)
  - Provides authorized access to resources as provisioned
  - Integrates business rules and assigned roles/access



Information Architecture: Where Does it Live?

	What	Where
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		



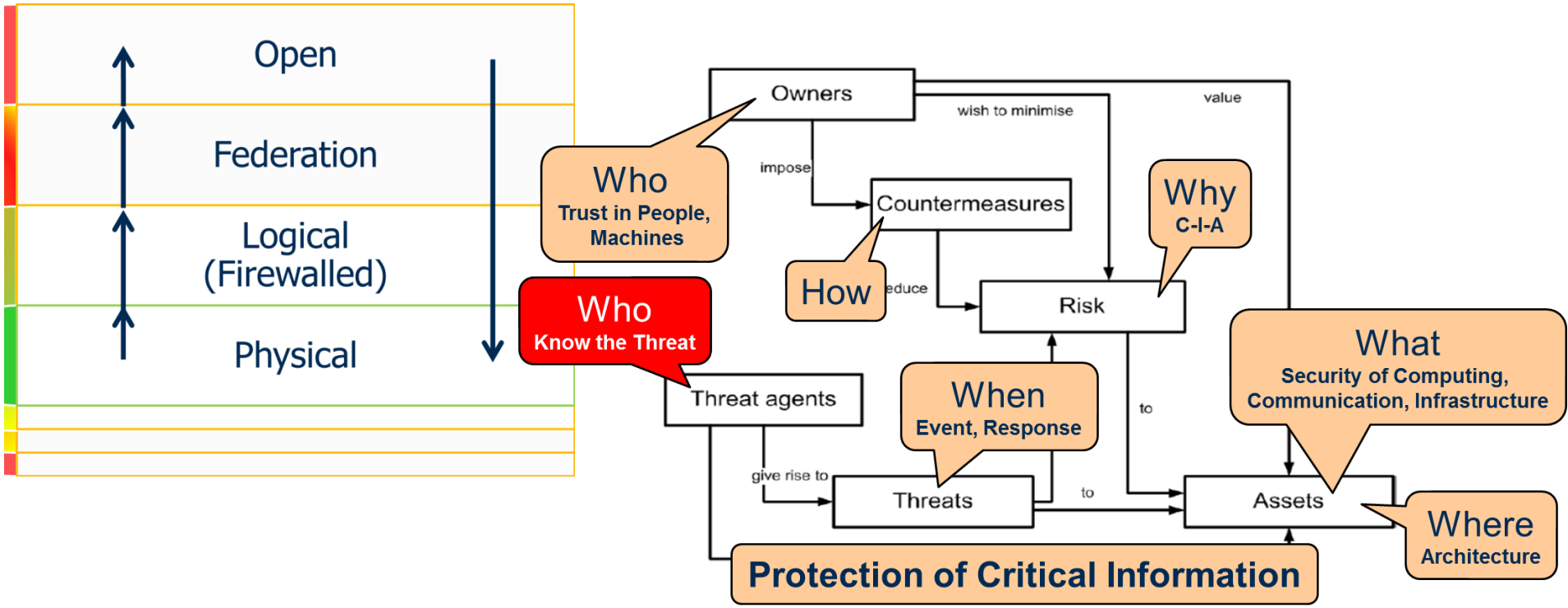
Data Architecture: Simplicity, Complexity, Resiliency

Security of Computing, Communication, Infrastructure

1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?

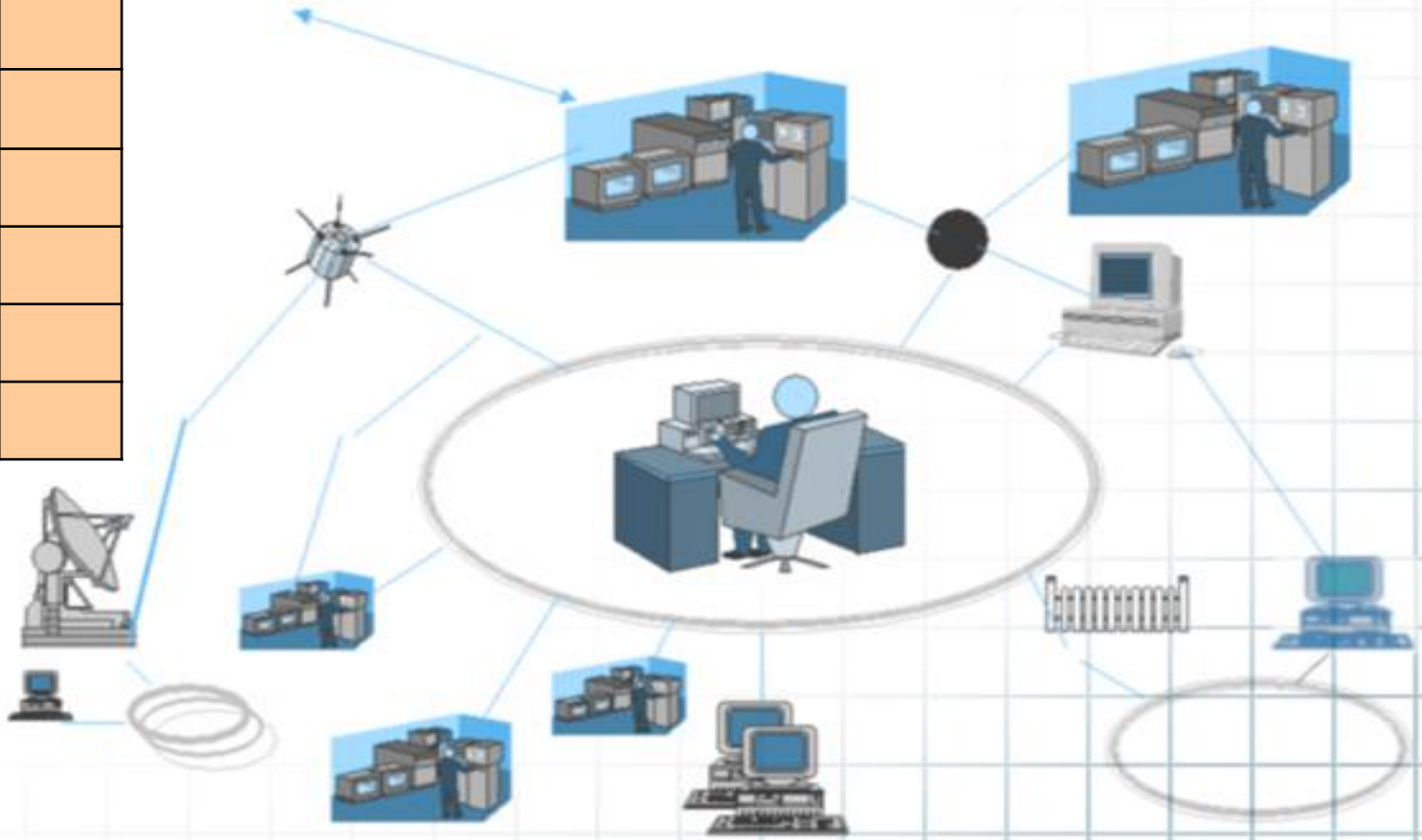
To Cloud or Not to Cloud

- Moves critical information to open or federated domains
- A good cloud is better than a weak local enterprise



OV-1 Data Network View

	Who	Where
Executive		
Business Process		
System		
Developer		
Operator		
Enterprise		



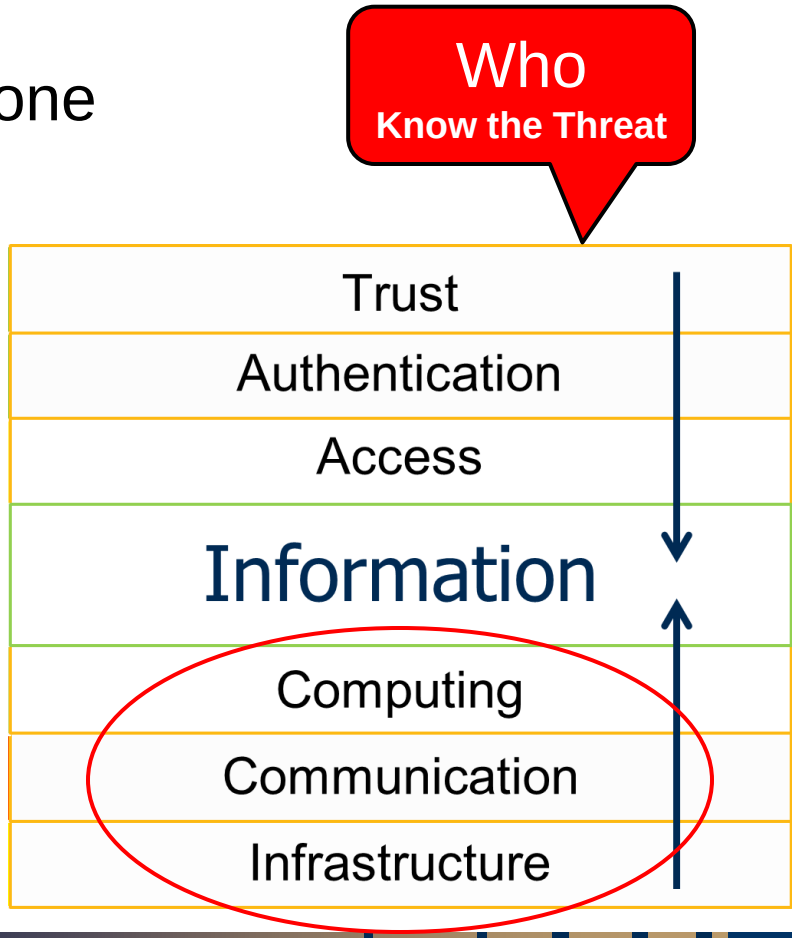
Trust in People, Machines (Software)

Security of Computing, Communication, Infrastructure

1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?

Wireless Problem Space

- Mobile phones limited by display size and computational limits (battery power)
  - Less user awareness of threat
- Wireless signals are visible to everyone
  - And could be interfered with by anyone
- Wireless networks eventually connect to wired networks
  - Subject to many of the same threats, plus many others
- Security involves both the networks and the “apps”
- Anyone can see anything you do on a mobile phone!

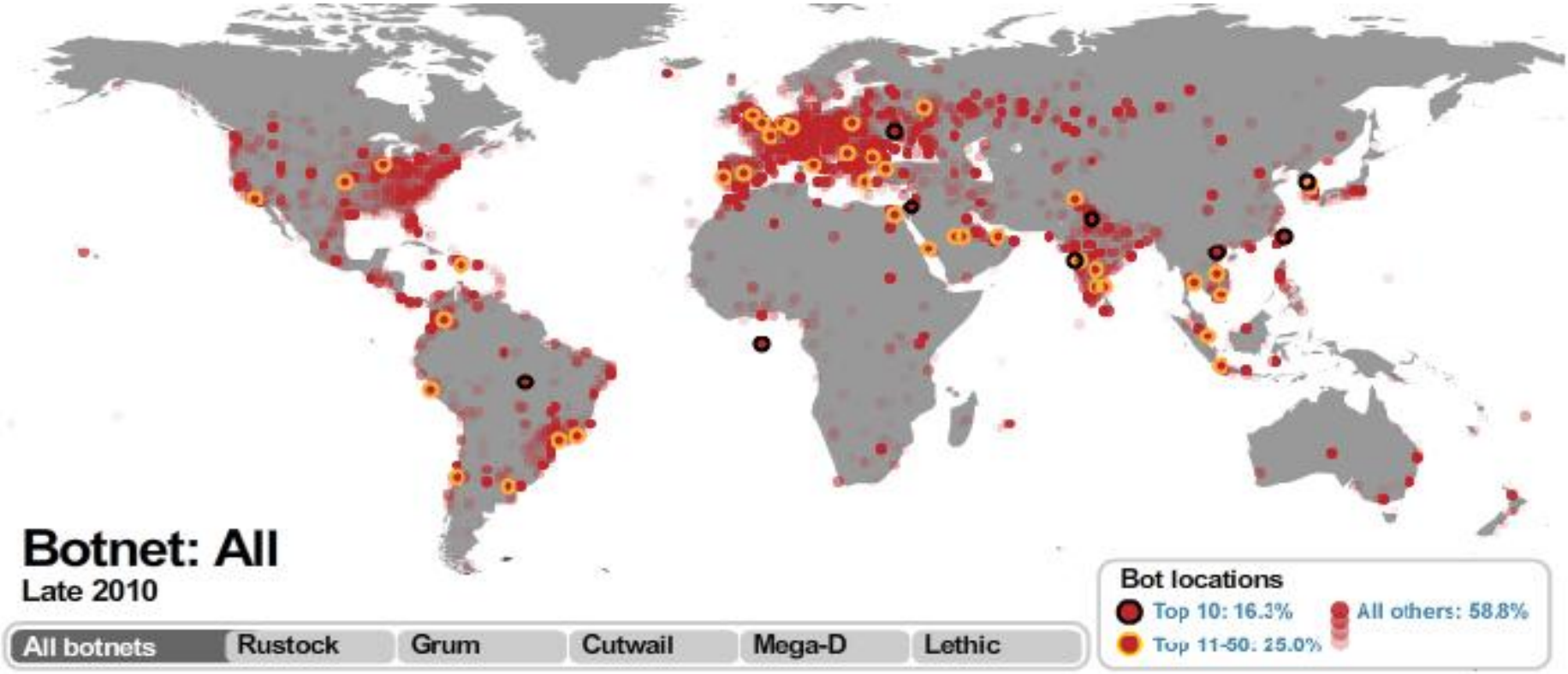


Example Quality Factors and Architectural Methods

- Safety
- Security
- Robustness
- Resiliency
- Availability
- Portability
- Reuse
- Openness
- Modifiability
- Testability
- Maintainability
- Separation, simplicity
- Abstraction, restriction
- Distribution
- Redundancy
- Health monitoring
- Virtualization
- Encapsulation
- Standardization
- Design rules, patterns
- Partitioning
- documentation

Denial of Service: Resiliency

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.



Reference: http://www.symanteccloud.com/en/gb/globalthreats/threatmaps/botnets

Reference: http://en.wikipedia.org/wiki/Denial-of-service_attack

Malware Defense: Awareness & Resiliency

- Significant Malware attacks require active response
  - Scanning, Isolating, Reconfiguring

Monthly Malware Statistics, February 2011

Share Print

February in figures

The following statistics were compiled in February using data from computers running Kaspersky Lab products:

- 228,649,852 network attacks blocked;
- 70,465,949 attempted web-borne infections prevented;
- 252,187,961 malicious programs detected and neutralized on users' computers;
- 75,748,743 heuristic verdicts registered.

Cybercriminals perfecting drive-by attacks

February saw considerable growth in the use of Cascading Style Sheets (CSS) that contain partial data for script downloaders, a new method for spreading malware that makes it much harder for many antivirus solutions to detect malicious scripts. This method is currently being used in the majority of drive-by download attacks and allows cybercriminals to download exploits to users' machines without those exploits being detected.

Drive-by attacks using this method involve redirecting users from an infected site to a page containing CSS data and a malicious script downloader, usually with the help of iFrame. Three infected pages of this type were among the Top 20 most malicious programs detected on the Internet in February: Trojan-

Author

Vyacheslav Zakorzhevsky

» All analysis articles

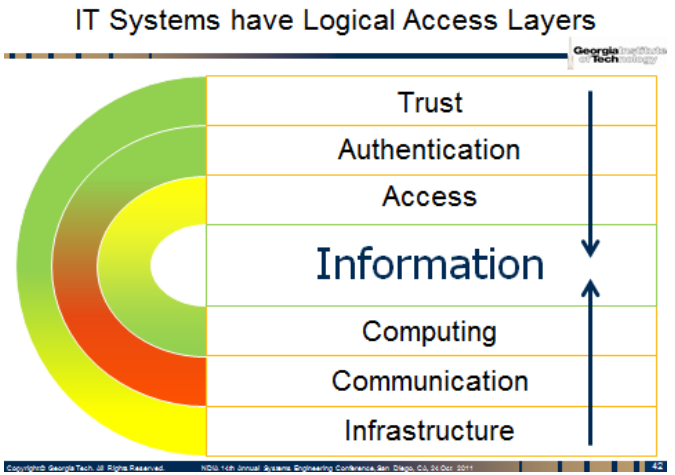
Analysis

» Monthly Malware Statistics: August 2011
» IT Threat Evolution: Q2 2011
» Monthly Malware Statistics: July 2011
» Monthly Malware Statistics, June 2011
» IT Threat Evolution for Q1-2011

Reference: http://www.securelist.com/en/analysis/204792185/Monthly_Malware_Statistics_July_2011

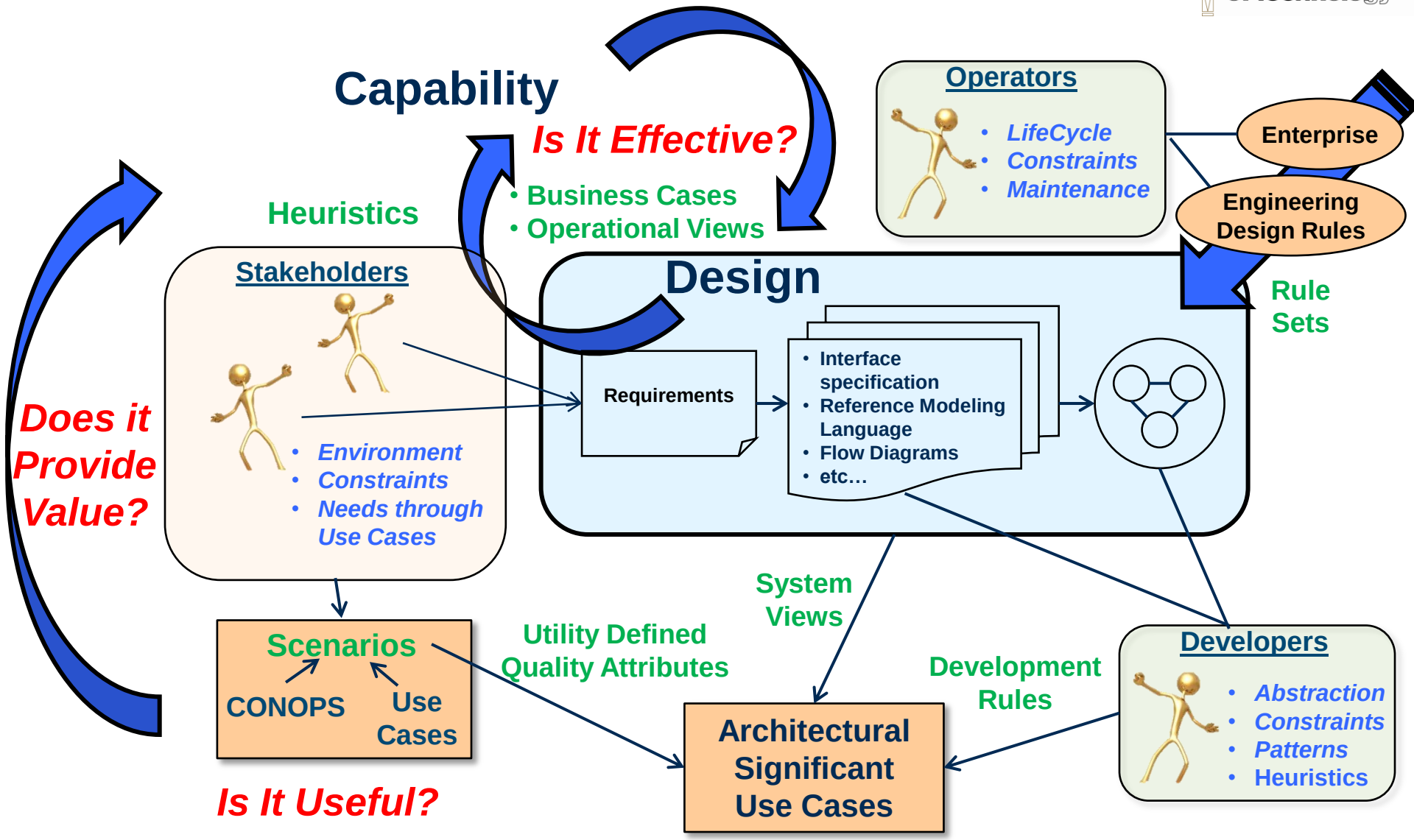
Example Public IT Security Framework

- **Business Aspiration:** Information Security Management Program
- **What:** Physical and Environmental Security
- **What:** Information Systems Acquisition, Development and Maintenance
- **What:** Communications and Operations Management
- **What, Who:** Human Resources Security
- **Why:** Risk Management
- **Where:** Asset Management
- **Where:** Access Control
- **When:** Business Continuity Management
- **How:** Security Policy
- **How:** Compliance
- **How, When:** Organization of Information Security
- **How, When:** Information Security Incident Management



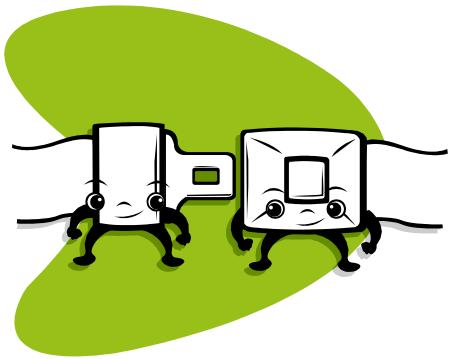
HITRUST Common Security Framework, Health Information Trust Alliance, http://www.hitrustalliance.net/

Perspective of the Systems Architect



Conclusion

- Introduction to Cyber Security
- Understanding the Threat
- Cyberspace as a Complex System
- Information Assurance
- Enterprise Architecture
- The System Architect
- Example Methods



Tutorial Objectives

- Introduce the concept of cyber defense and the need for system engineering approach
- Introduce the cyber threat (attacker) and information assurance (defender)
- Characterize cyber defense as a complex system
- Introduce methods, processes, and tools for managing cyber defense within an enterprise architecture

What is Not in This Tutorial

- Legal, regulatory, operational constraints
- A complete enterprise framework
- IT System description and design methods
  - High Level Curricula: Days
  - Detailed Curricula: Weeks
- Detailed Modeling Methods
- Evaluation, Certification and Accreditation
- Methodologies for Cyber Defense in IT systems
- Incident Response planning and operations

The **Georgia Tech Information Security Center** and the **Georgia Tech Research Institute** provide a comprehensive set of academic, professional, and executive curricula from one of the leading security research and education programs in the world

Primary References*

- The Common Criteria for Information Technology Security Evaluation, http://www.commoncriteriaportal.org.
- IEEE-STD-1471-2000, “Systems and software engineering —Recommended practice for architectural description of software-intensive systems”
- Tom Graves, Bridging the Silos: Enterprise Architecture for the IT Architect, Tetradian Books, December 2008, ISBN: 978-1-906681-02-9.
- The Open Group Architecture Framework, TOGAF version 9, 2009.
- The Zachman Framework for Enterprise Architecture, Zachman International, www.zachman.com.
- Test and Evaluation of Cyber Systems, Georgia Tech Tutorial, 2011.

*** Other references used in this tutorial are cited on appropriate slides**