Internet and Internet Communication(s)

June 2012

The views expressed in this presentation are those of the authors (CSFI managers and Paul de Souza, CSFI founder) and do not reflect the official policy or position of any US government agency, department, or service, or any other entity operating under the authorities or statutes of the U.S. government or any other government the U.S. does or does not recognize.

This presentation's facts, information, and data contained herein are sourced from the public domain.

Course Description

- The student will be introduced to the concept of "Cyberspace"
- The course will introduce the student to the concepts, architectures and technologies supporting Internet-related computer network operations.
- This course covers computer network defense and attack vectors that could be utilized by an adversary.
- The student will expect to learn about Defense-In-Depth strategy and how this can be applied to computer network defense by exploring real life and historical examples.
- The student will also study the various layers that comprise the Defense-In-Depth strategy

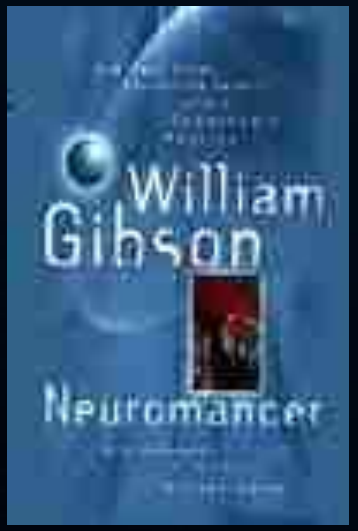
Course Goals

- To increase understanding about the underlying concepts, architectures, and technologies that enable computer network operations.
- To increase understanding about computer network defense as it relates to computer network operations from monitoring to analysis, detection and response.
- To increase knowledge about computer network attacks in regards to computer network operations.
- To increase knowledge of the layered approach of Defense-In-Depth based on the principles of a solid information assurance posture.
- To increase understanding in regards to information assurance as it pertains to network attacks and network defense measures.

Agenda

- What is "Cyberspace"
- Cyberspace and computer network operations
- Introduction to networking concepts, architectures and technologies supporting Internet-related computer network operations
- Computer network operations and computer network defense
- Defense-in-Depth (DID)
  - Various Layers/Elements of DID
- Ensuring DID
- Integrating Information Assurance into Environment
- Discussion Questions
- Summary and Sources

Cyberspace



“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...”

William Gibson, *Neuromancer* , 1984

What is Cyberspace?

"Man-made"-domain:

- Operations (i.e., computer network operations (CNO)) analogous to operating in air or maritime domain

- Cyberspace is *"a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."*

Daniel T. Kuehl
"From Cyberspace to Cyberpower: Defining the Problem"
Cyberpower and National Security, NDU Press, 2009

- Networks, including hardware & software are militarily relevant- their counterparts in other domains: ships, vehicles, airplanes & satellites

- Cyberspace traverses the physical domains or land, sea, air, and space through interconnected technological devices.

OSI verses TCP/IP models

Applications (Data)

(Data)

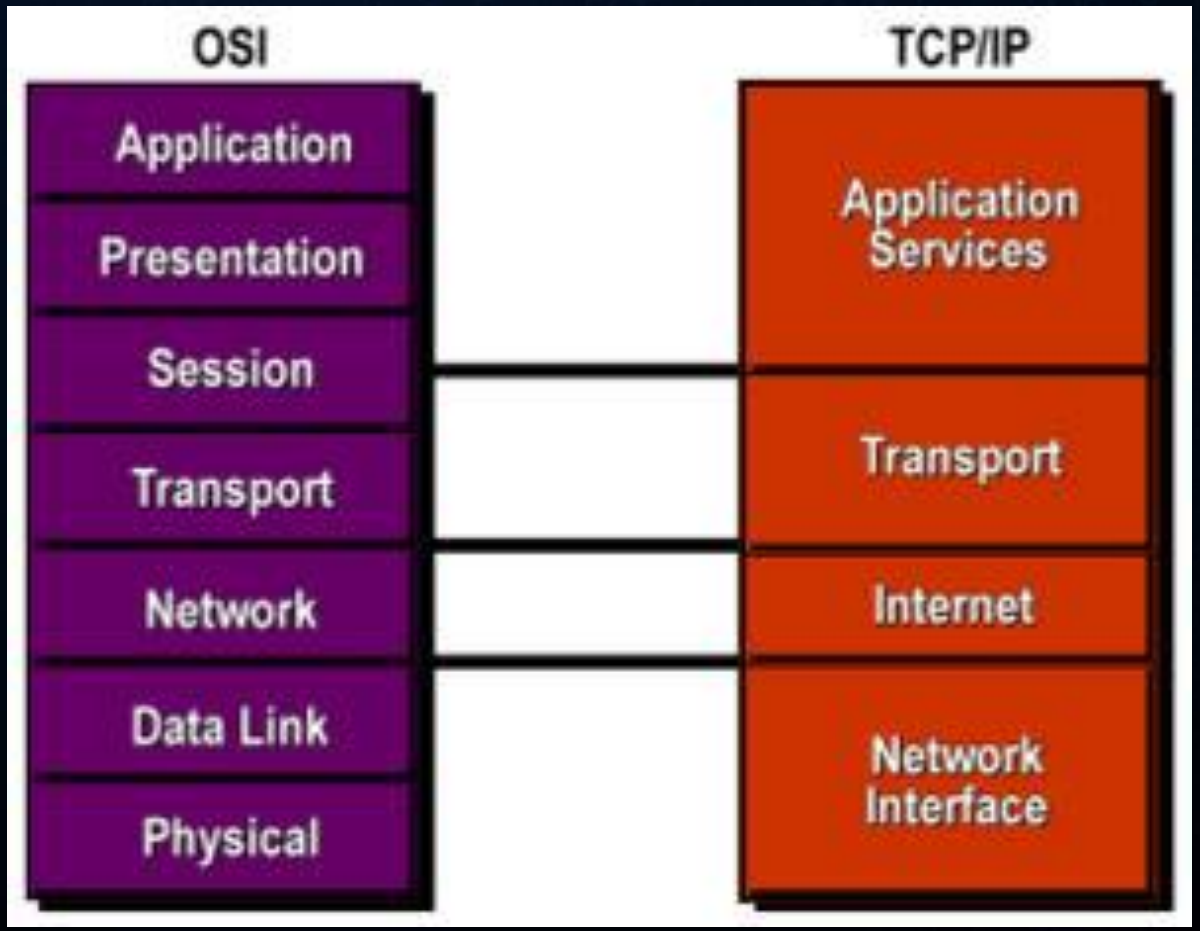
(Data)

(Segments)

Router (Packet/Datagram)

Switch/Bridge (Frame)

Hub (Bit)



Information Assurance (IA)

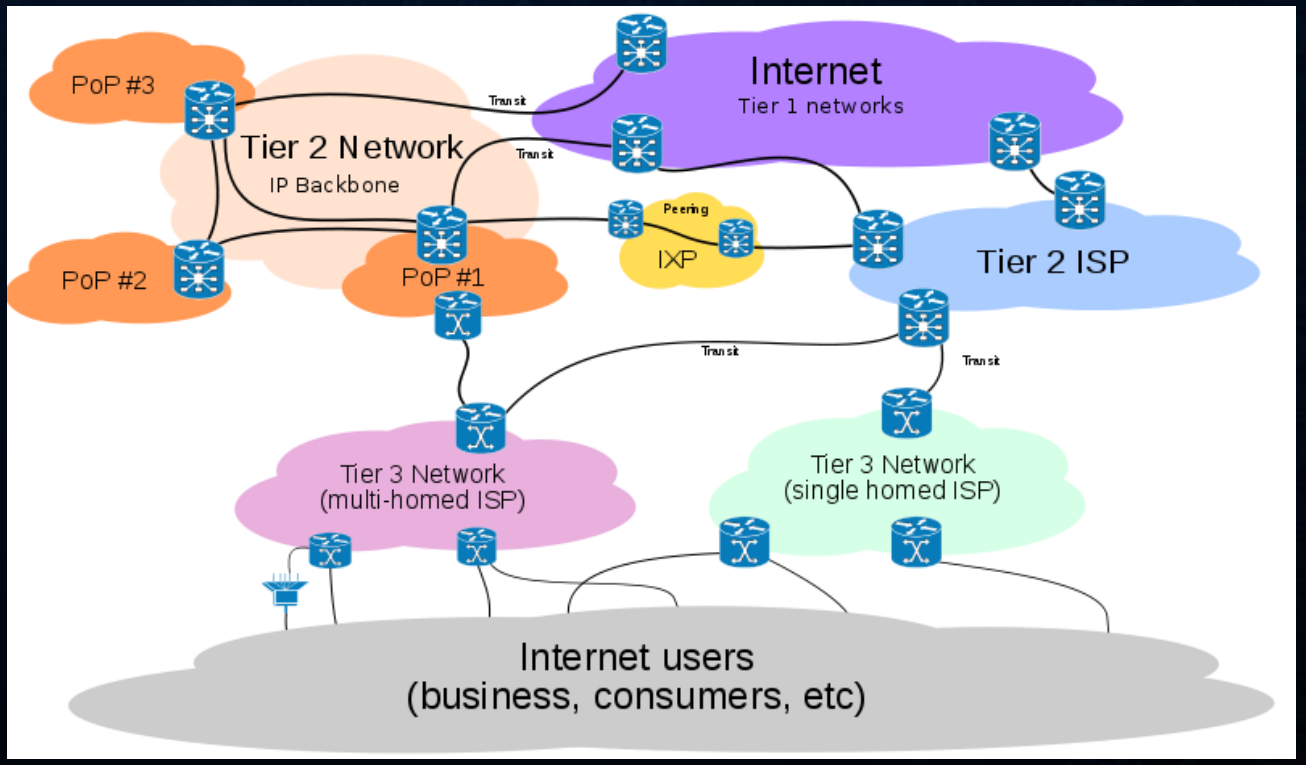
- Confidentiality
- Integrity
- Availability

Internet Service Provider (ISP)

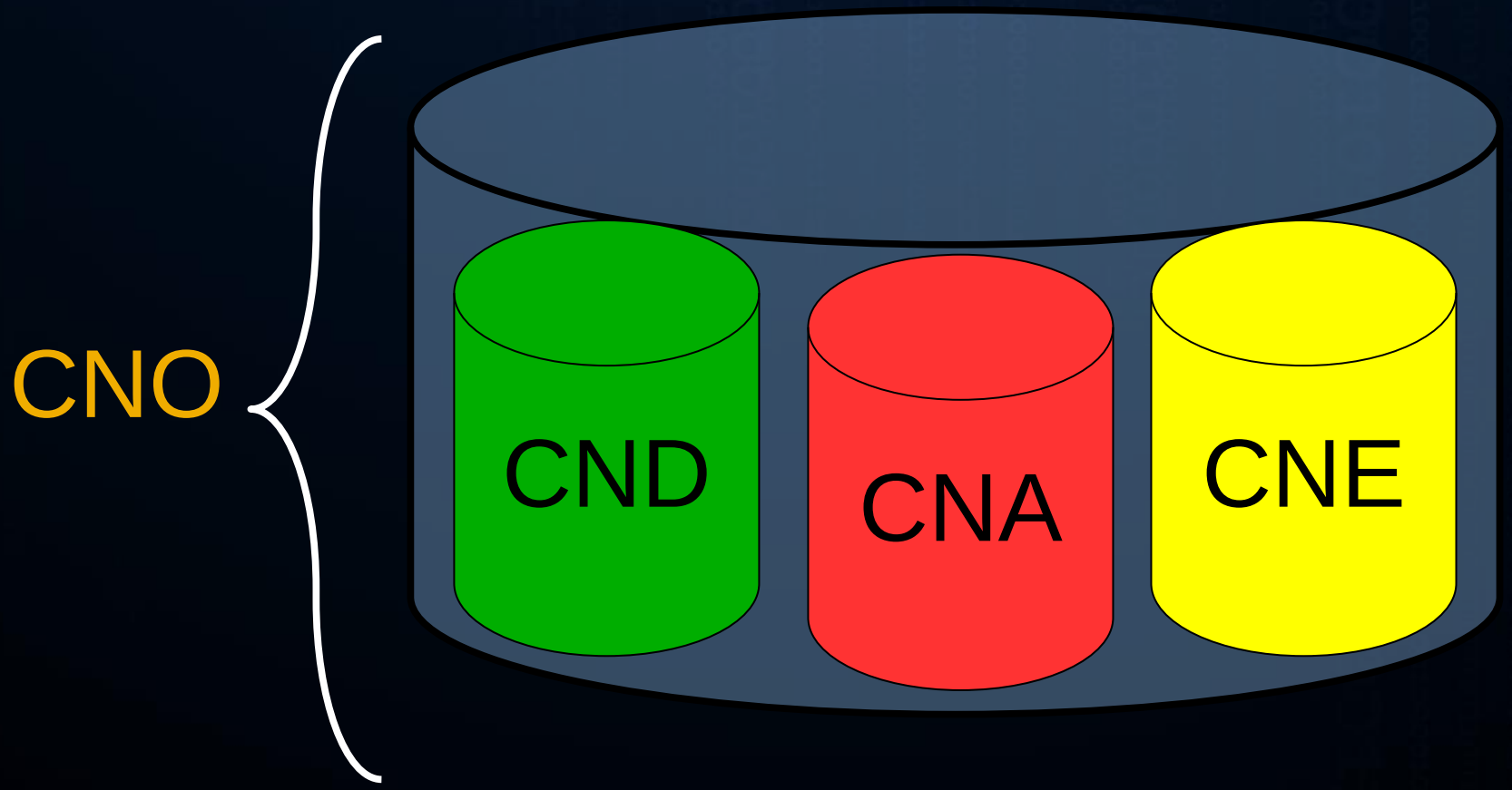
- Tier-1: transit-free network that peers w/ every other Tier-1 network

- Tier-2: a network that peers w/ some networks but purchases IP transit or pays settlements to reach some portion of the Internet

- Tier-3: a network that solely purchases transit form other networks to reach the internet



Computer Network Operations



Computer Network Operations (cont'd)

- "Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations."

Computer Network Attack

- "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"

Outside of the Scope of this Course

Computer Network Exploitation

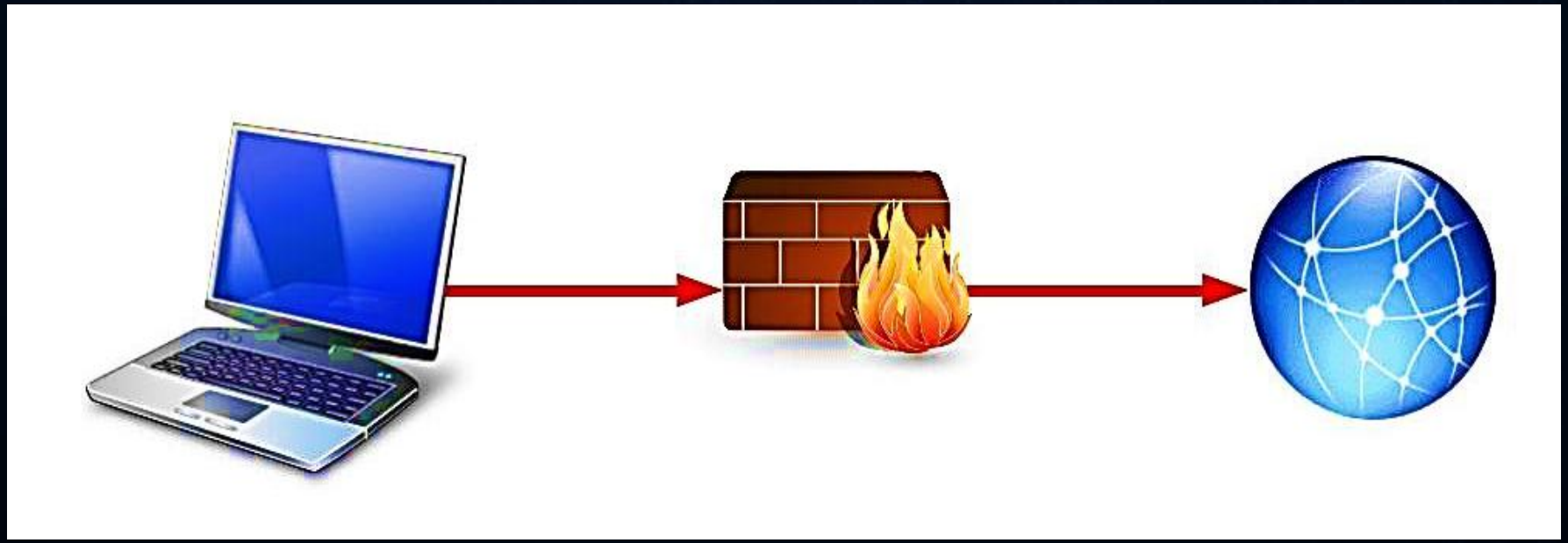
- "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks"

Outside of the Scope of this Course

Computer Network Defense

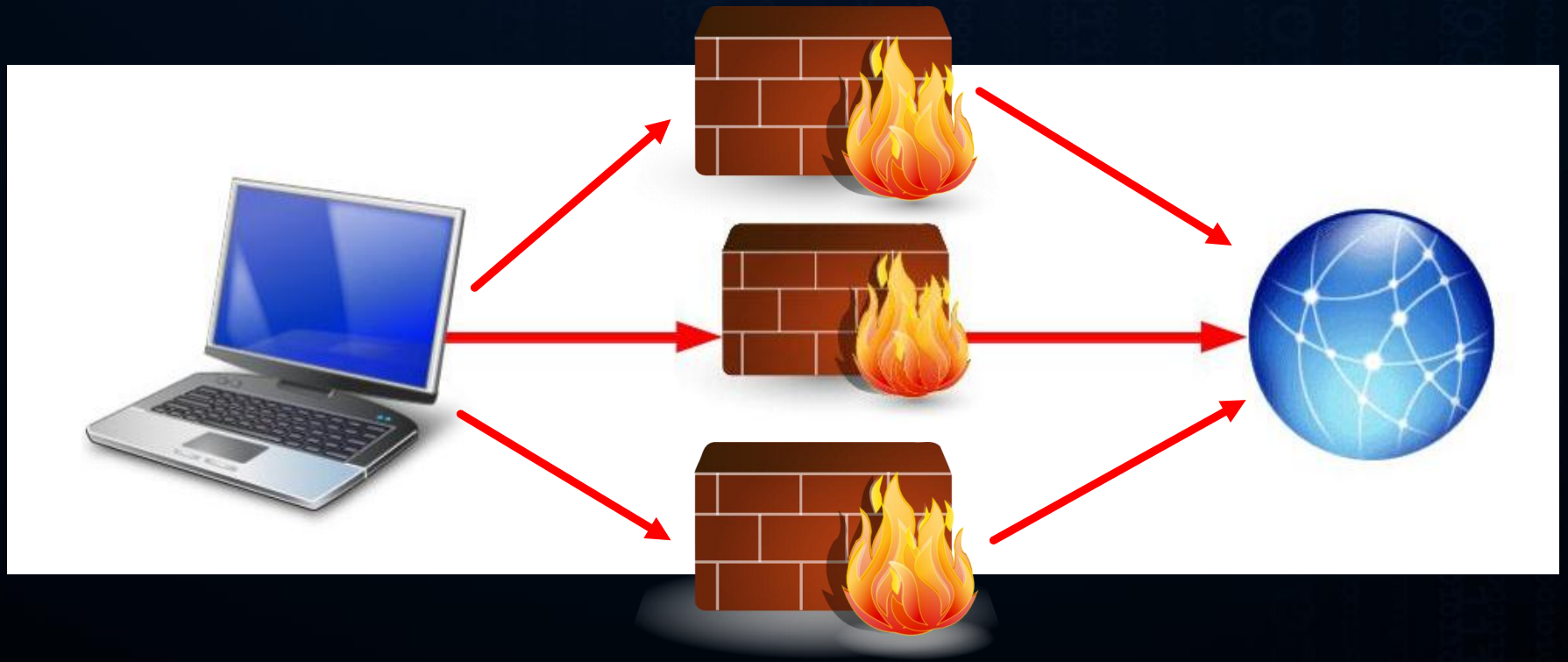
- "Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within…information systems and computer networks"

What CND is Not



Why?

Neither is This



Why?

Discussion Questions

- Is a network/system a weapon?
- What are the ramifications of using non-lethal systems in a way that could BE lethal?

Defense-In-Depth

- "The sitting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver the reserve"
  - Source: Department of Defense
- Putting that idea into a cyber context…

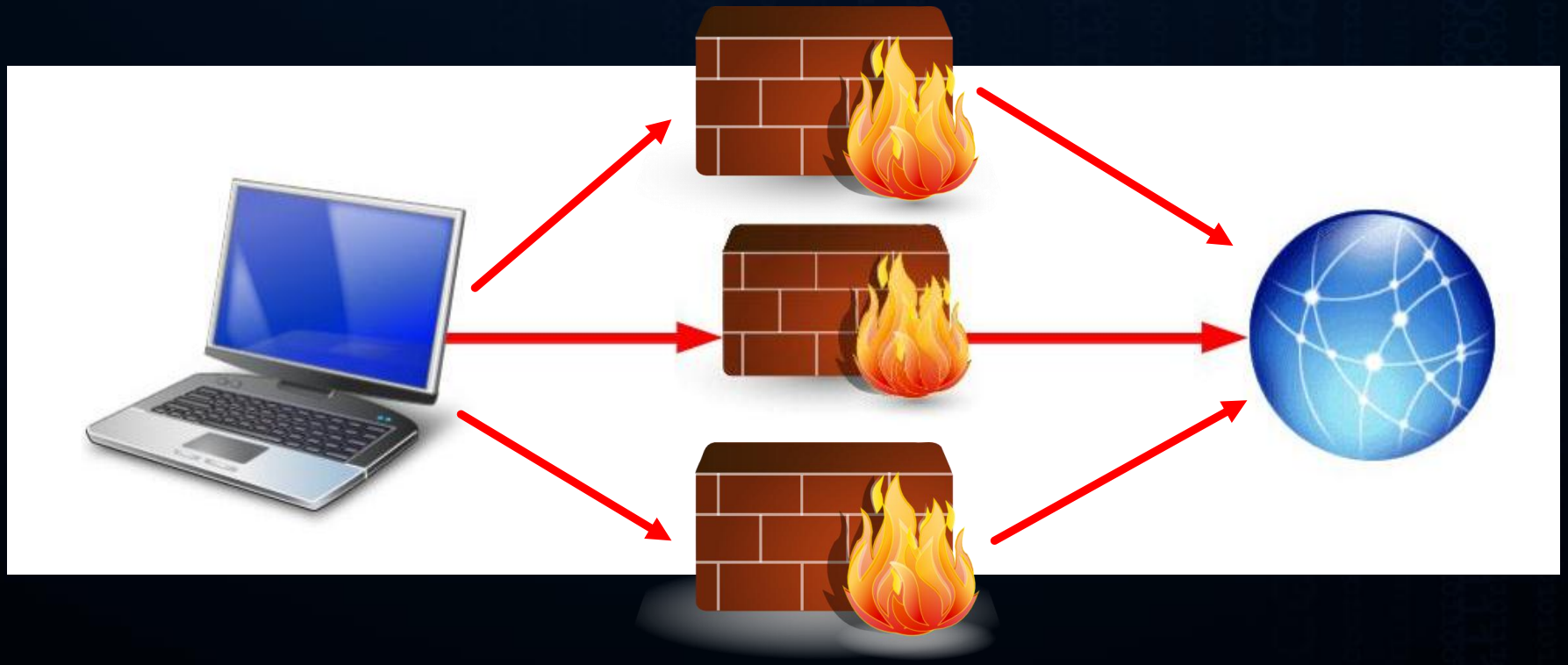
In More Detail

- Three Core Components
  - People
  - Technology
  - Operations
- Not the same as redundant elements
  - Having multiple firewalls does not provide DID
    - Just like having a single firewall does not equate to CND
- Each element in a DID strategy must compliment the other elements

Examples

- Using more than one of the following layers constitutes defense in depth.
- Physical Security
- Authentication and password security
- Hashing passwords
- Anti virus software
- Firewalls (hardware or software)
- DMZ (demilitarized zones)

Remember This?



People

- Security Architects
- Security Engineers
- End-users
- CND Operations Staff
- Network Technicians
- Security Analysts
- Informed Leadership
  - This is the most critical mission of IA

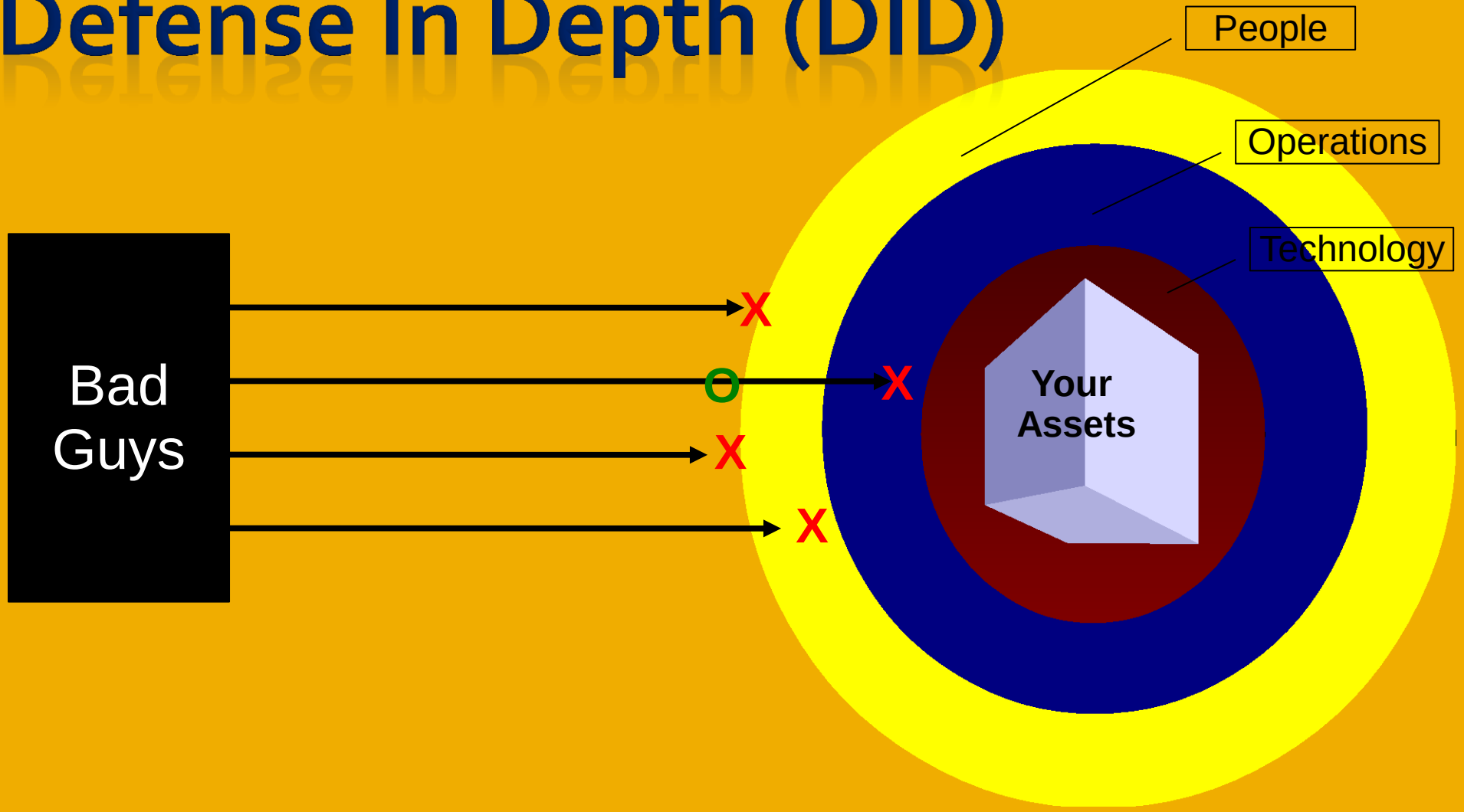
Technologies

- Evaluated products
  - Common Criteria
- Configuration management systems
- Firewalls
- Perimeter defense systems
- Access control systems
- Proxy Servers
- Content filtering software
- Hardened/patched operating systems
- Encryption mechanism
- Authentication system

Operations

- Security policy
- Standard operating procedures
- Business continuity plans
  - Disaster Recovery
  - Continuity of Operations
- Configuration Control Boards
- Incident response processes
- Forensics capabilities
- Security training
- Security as a culture

Defense In Depth (DID)



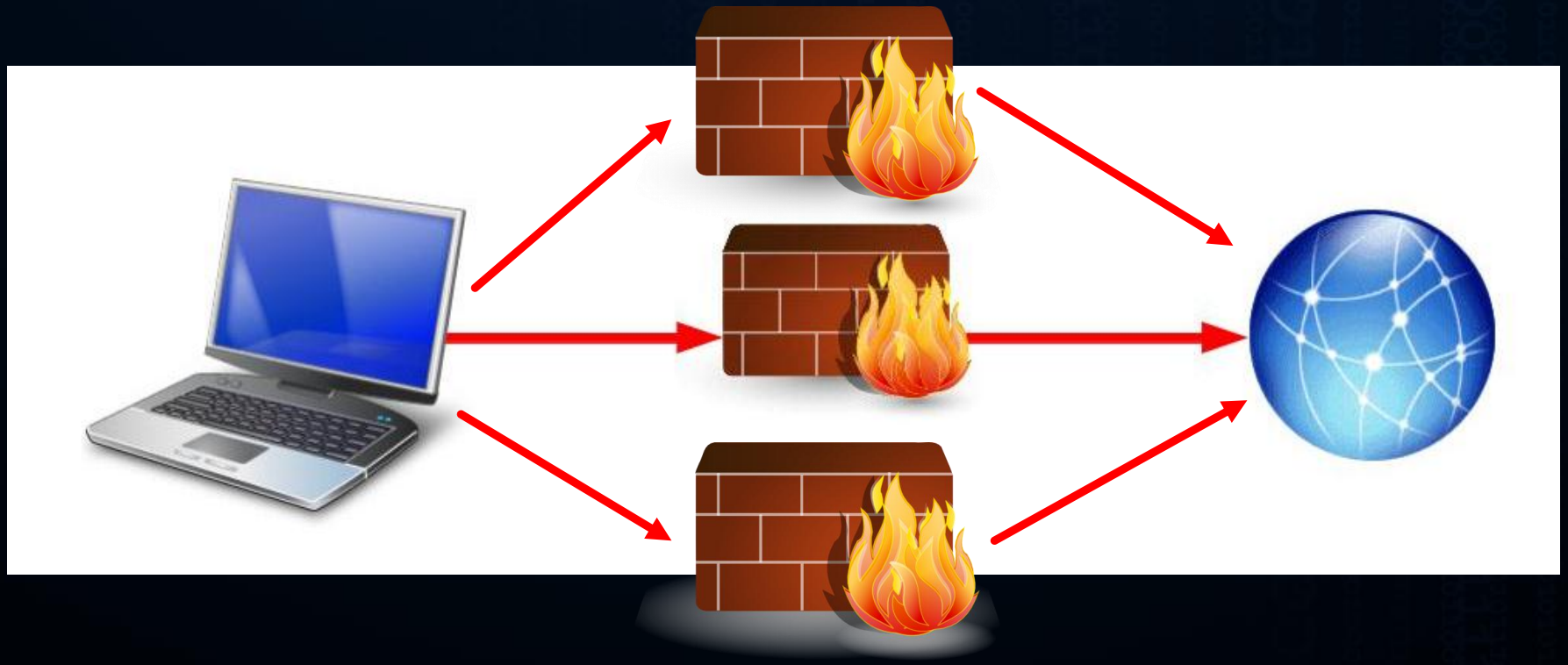
A Possible Concern?

- "DID can provide robust information assurance properties; however, we must consider whether layers of defense may result in delaying potential compromise without providing any guarantee that compromise will be completely prevented."
  - Networking and Information Technology Research and Development (NITRD) Program

Said Another Way

- “It is not accurate to say 'more depth equals more security'”
  - Robb Reck, CISSP, CRISC

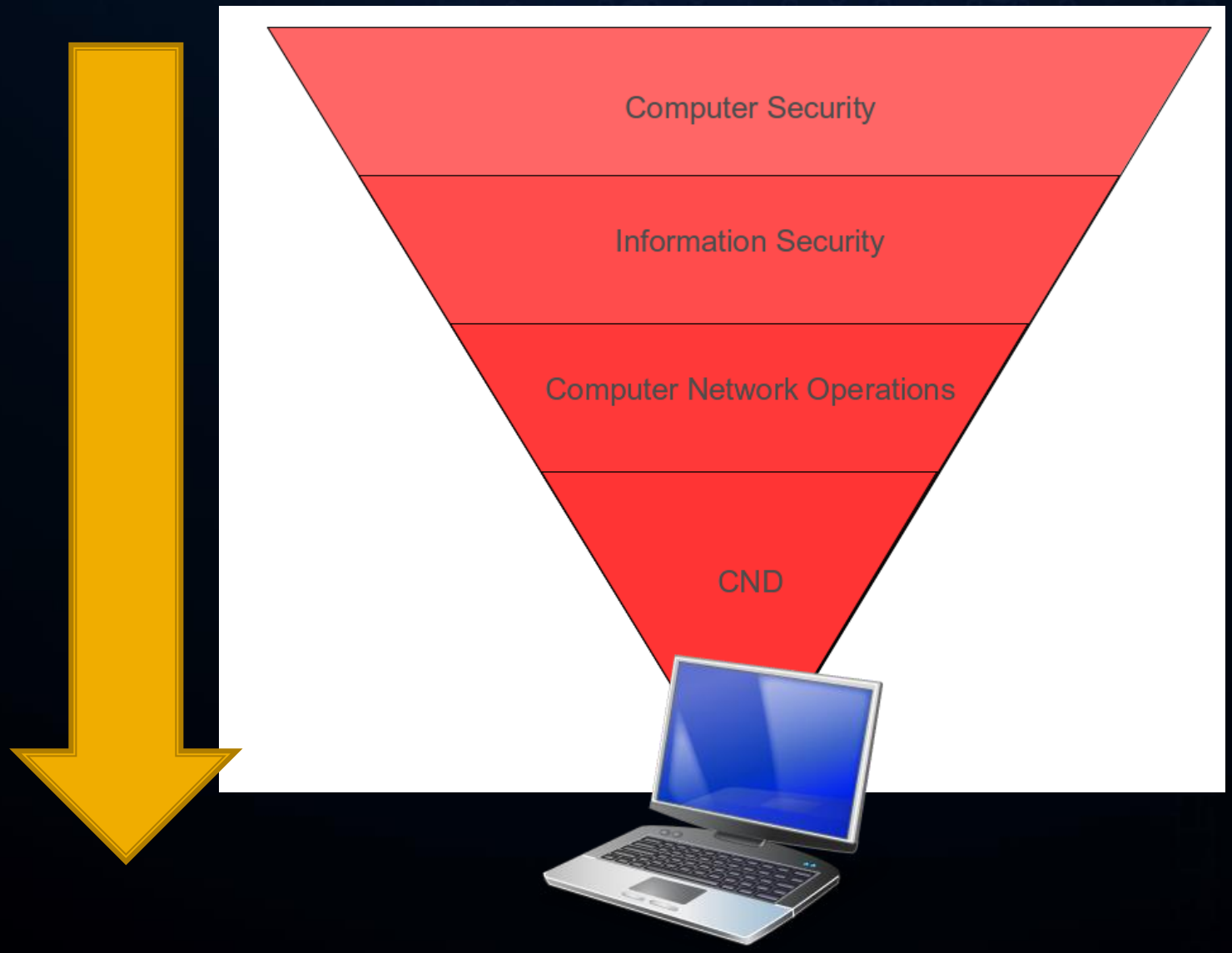
Remember This?



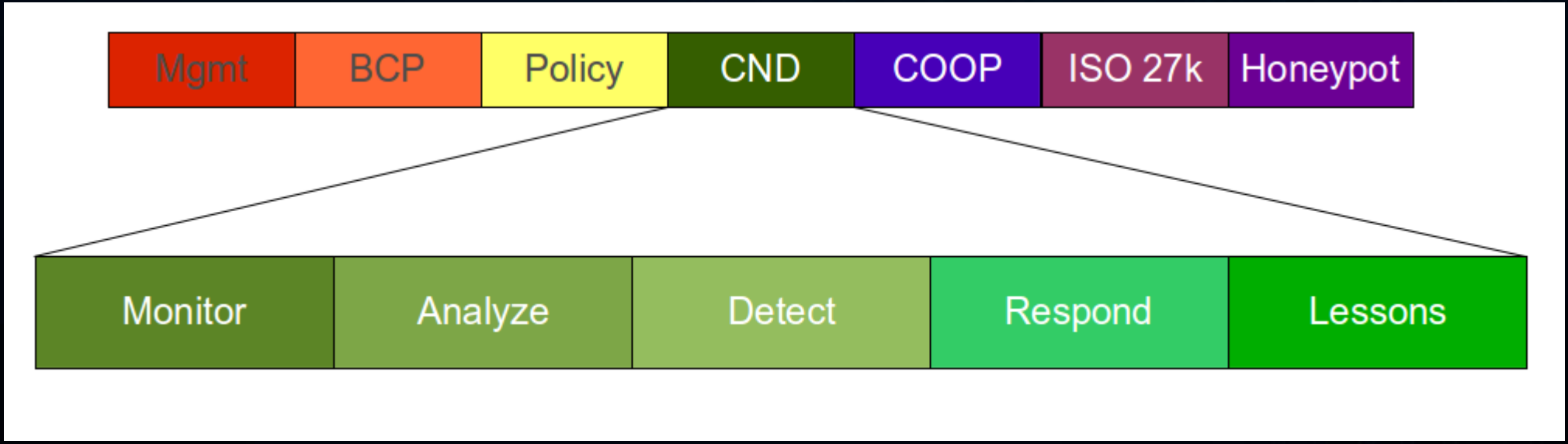
Information Assurance

- "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."
- Compare that to Computer Security
  - "The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems."
  - Differences?
  - Commonalities?

Flowing Down



CND and DID: The Marriage



Discussion Questions

- Why is CND considered critical but CNA is not?
- Is a security policy control fall into the people or the operations category?
- What is the weakest link in the CND triad?

DID Layers

Internet Grid

WAN

LAN

End-User Environment

Data Integrity

Internet Grid

- Routers
- Cables
- Servers
- Copper
- Email
- Fiber Optic
- DNS

Wide Area Network (WAN)

- Routers
- Cables
- Servers
- Copper
- Email
- Fiber Optic
- DNS
- Firewalls

Local Area Network (LAN)

- Routers
- Servers
- Hubs
- Switches
- Firewalls

End-User Environment

- Desktops
- PCs
- Laptops
- iPads
- Smart Phones
- User Training

Data Integrity

- Encryption
- Hashing

Discussion Questions

- What different controls are in place between routers in the LAN space versus the Grid space?
- How have open standards improved the security of networks and systems?

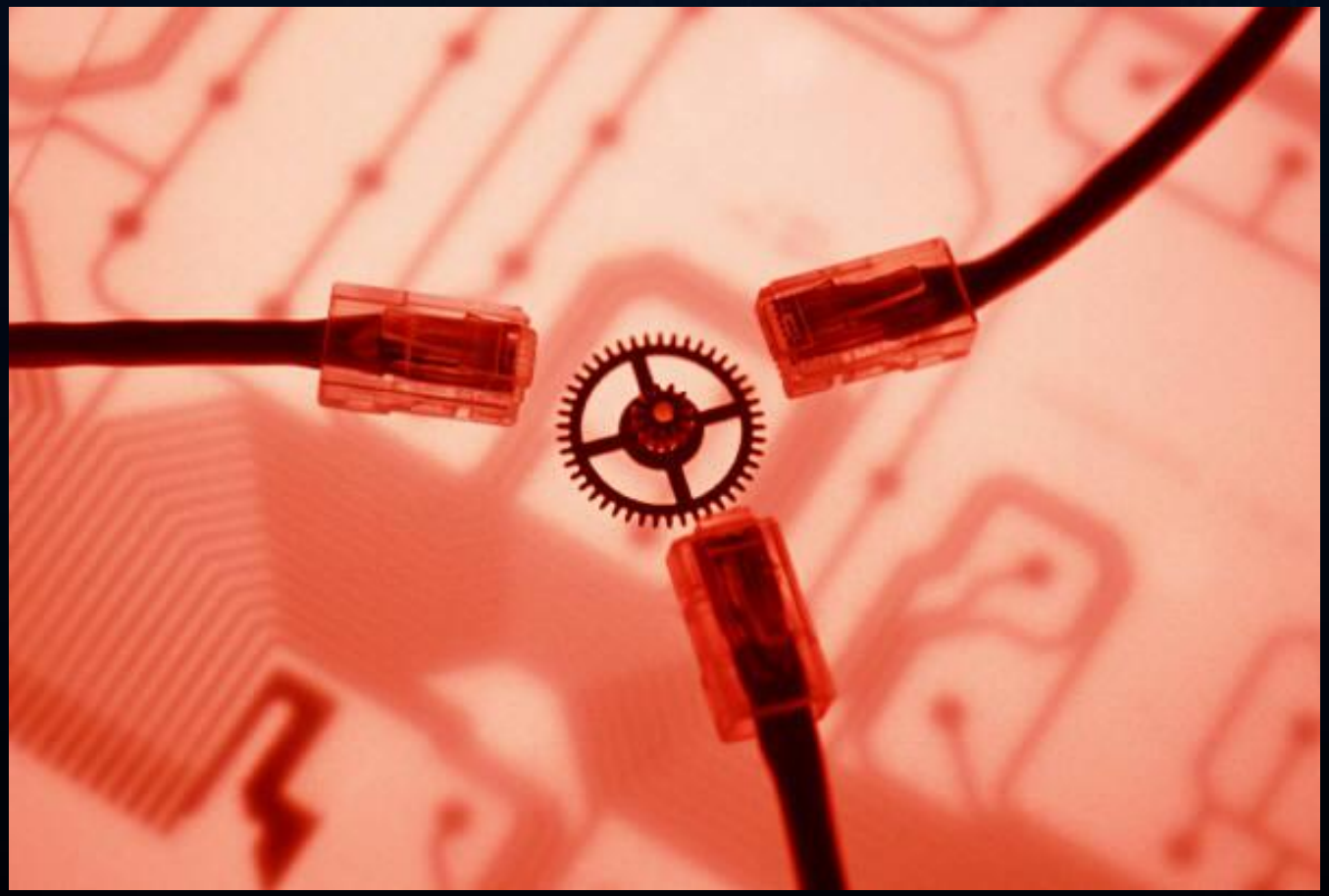
Ensuring CND

The Process


Detecting
Automated Tools
Analyzing
What is Abnormal?
Event vs. Incident
Responding
Investigation
Containment
Eradication
Lessons Learned
Often Overlooked

Lessons Learned

Integrating IA into the Environment



Eggs and Basket Conundrum

Get (Demand) Better Products

Common Criteria

DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND

ICSA labs
An Independent Division of Verizon Business

Discussion Questions

- Which approach presents the best scenario for cost savings?
- Why?

Discussion of Real-world Examples

- Epsilon (2011)
- Michael Calce (2000)
- Titan Rain (2004)

"10 Most Costly Cyber Attacks in History | Business Pundit." *Business Pundit*. SeaWaves Technology, 15 Aug. 2011. Web. 26 Oct. 2011. <http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/>.

Epsilon

- Data Breach of firm that provides marketing and email handling for Fortune 500 companies

Michael Calce

- MafiaBoy

Titan Rain

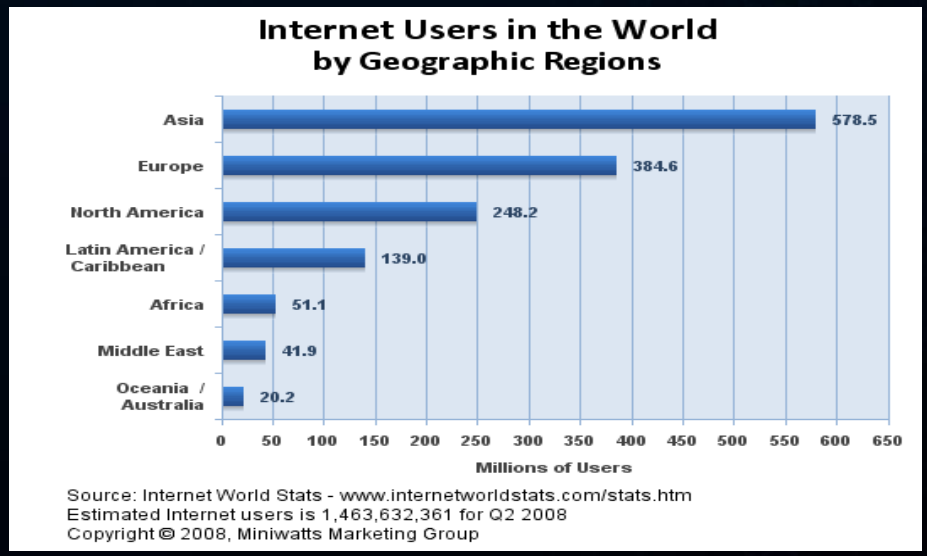
- Designation by FBI for series of computer intrusions for US Government/Defense Industrial Base (DIB) systems

Cyber Truisms

- Industry drives cyberspace technology
- We operate and defend on the same platform(s) as the adversaries
  - Threat characterization and attribution are challenging
  - Offense and defense have similar features
- Public, high profile adversary successes will breed additional actors
  - Inexpensive, anonymous and effective

Cellular Expansion

Internet Explosion



Discussion Questions

- How could a solid DID foundation have prevented each of these examples?
  - Is it even possible to prevent them?
- General Discussion, e.g., Cyber Truisms

Review of Course Goals

- To increase understanding about the underlying concepts, architectures, and technologies that enable computer network operations.
- To increase understanding about computer network defense as it relates to computer network operations from monitoring to analysis, detection and response.
- To increase knowledge about computer network attacks in regards to computer network operations.
- To increase knowledge of the layered approach of Defense-In-Depth based on the principles of a solid information assurance posture.
- To increase understanding in regards to information assurance as it pertains to network attacks and network defense measures.

Bibliography

- William Gibson, “Neuromancer”, Ace Science Fiction, 1984
- Daniel T. Kuehl. “From Cyberspace to Cyberpower: Defining the Problem”Cyberpower and National Security, NDU Press, 2009
- “Tier 1 network." Wikipedia, the Free Encyclopedia. Web. 26 Mar 2012. <http://en.wikipedia.org/wiki/Tier_1_ISP/>.
- Batie, Robert B. "Requirements Analysis and Security Standards/Guidelines Criteria." Official (ICS2) Guide to the CISSP-ISSAP Access Control Systems and Methodologies. Print.
- "Cyberspace Operations." DTIC Online. Web. 30 Mar. 2011. <http://www.dtic.mil/doctrine/dod_dictionary/data/c/20173.html>.
- "Cyberwarfare." Wikipedia, the Free Encyclopedia. Web. 30 Mar. 2011. <http://en.wikipedia.org/wiki/Cyber_warfare>.
- Price, Sean. "Access Control Systems." Official (ICS2) Guide to the CISSP-ISSAP Access Control Systems and Methodologies. Print.
- Reck, Robb. "Defense in Depth Is Necessary, but Not Sufficient." InfoReck. Web. 30 Mar. 2011. <http://www.robbreck.net/blog/enterprise_information_security/defense-in-depth-workshop/>.
- Covert, Edwin B. “GIAC Advance Incident Handling and Hacker Exploits Track Practical for Option 1 – Illustrate an Incident”. Published for SANS certification. Print.
- Powner, David A. "Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability." U.S. Government Accountability Office. U.S. Government Accountability Office, 31 July 2008. Web. 30 Mar. 2011. http://www.gao.gov/products/GAO-08-588.

Bibliography (con'td)

- "Taxonomy of the Computer Security Incident Related Terminology." TERENA. Web. 20 Mar. 2011. <http://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html#Appendix.>.
- "Cyber Solutions." Global InfoTek, Inc. (GITI). Web. 30 Mar. 2011. <http://www.globalinfotek.com/COE_cyber_Solutions.htm>.
- Forrest, Stephanie, Anil Somayaji, and David Ackley. "Building Diverse Computer Systems."