Information Security Principles

Kitisak Jirawannakool

Information Security Specialist

Agenda

- What is Security?
- Risk Analysis
- Incident Handling

How it used to be?

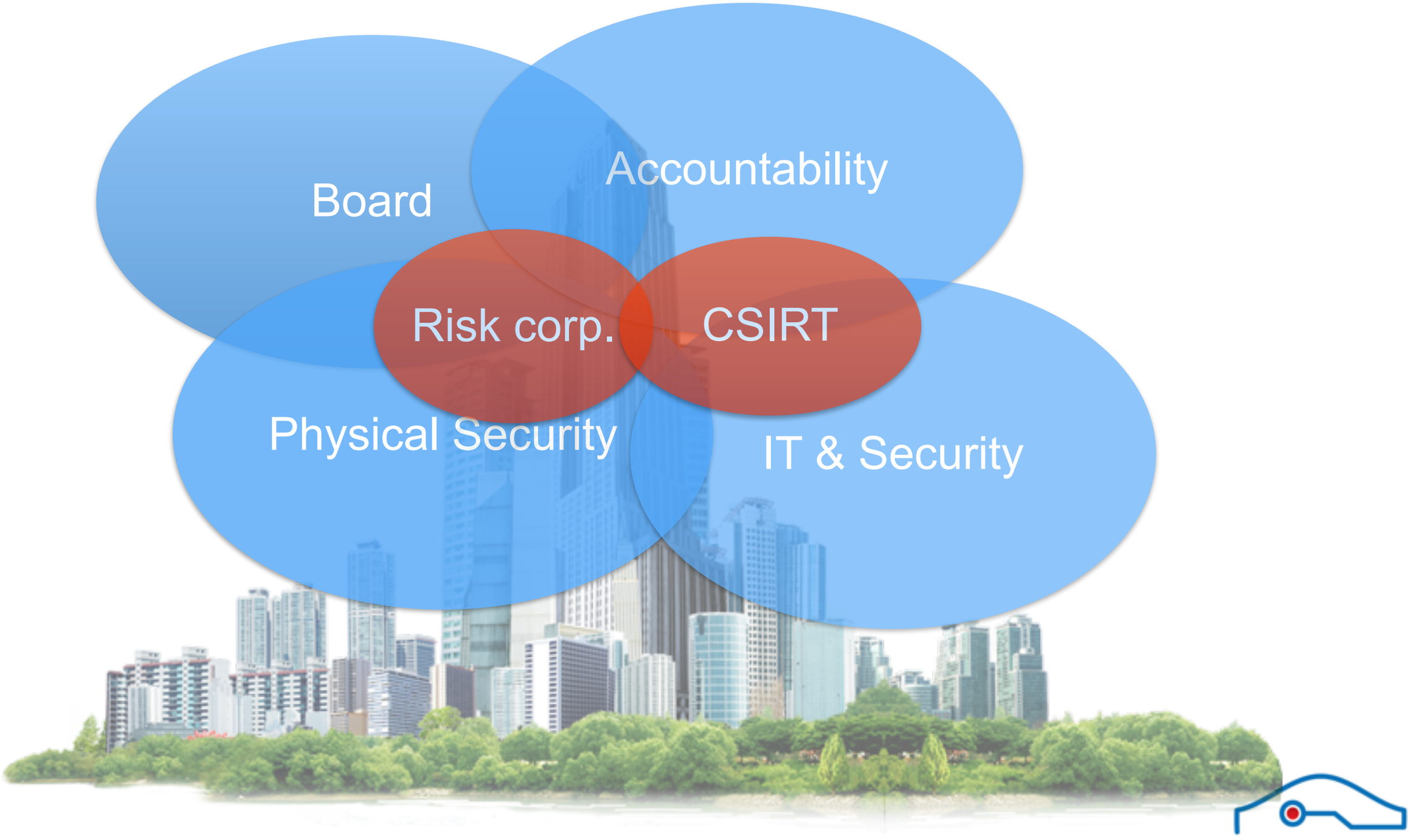
Board

Accountability

Physical Security

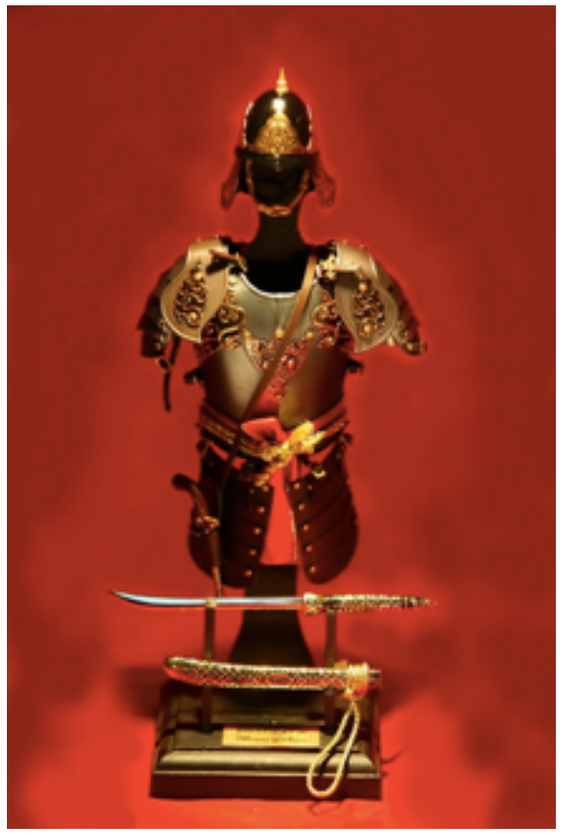
IT & Security

… and How it is growing to be?



What are we protecting?

- What is there to protect ?
  - Primary process
  - Customers, Employees, Identities
  - Products, Contracts
  - Supporting processes
  - Reputation
  - Information, infrastructure
  - Critical infrastructures
  - Health, lives



EGA
e-Government Agency

G-CERT by EGA

Assets

- Hardware
- Software
- Information
- Personnel (People)
- Service
- Location

What is Security?

What is security?

What is security?

What is security?

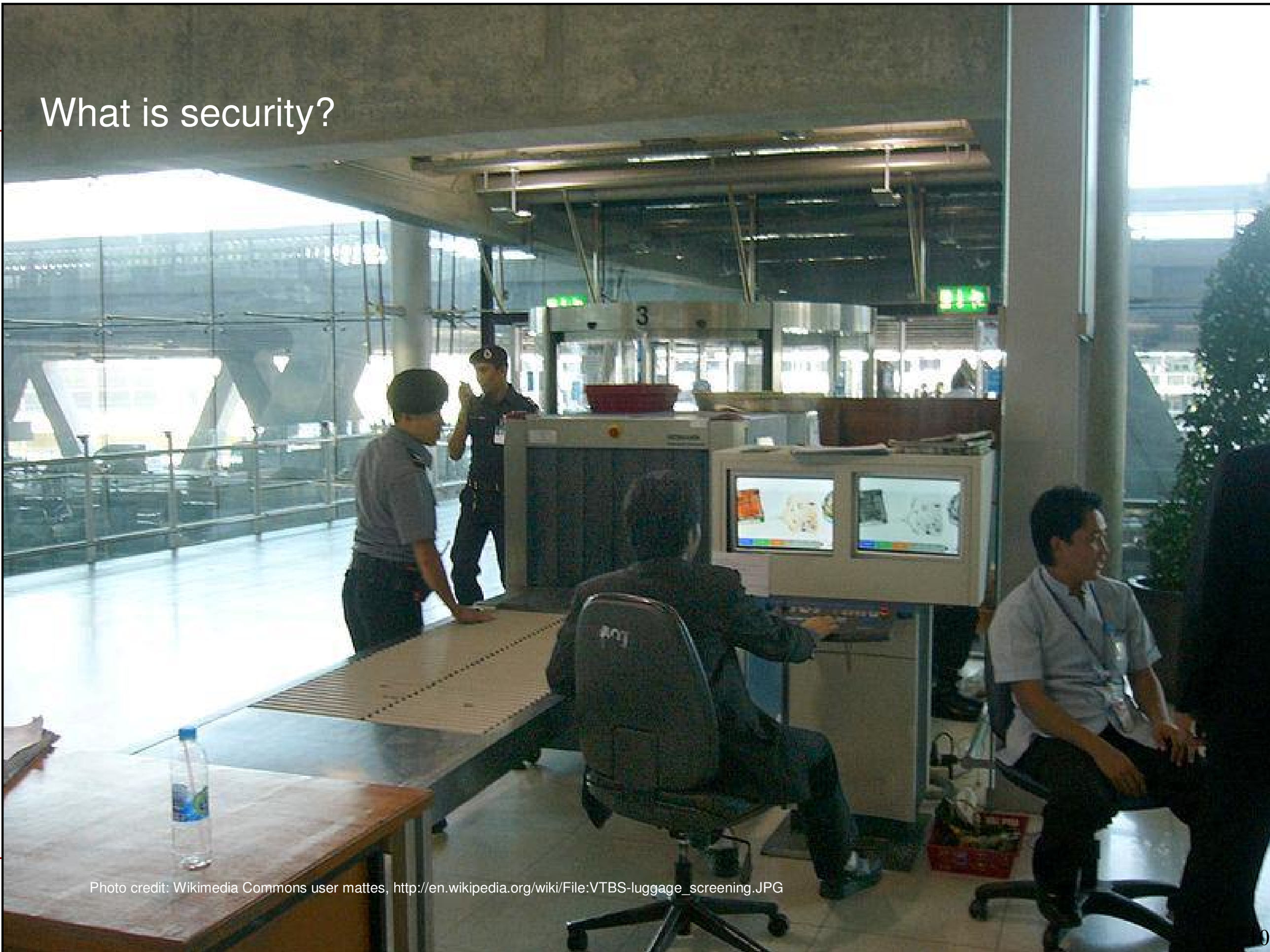


Photo credit: Wikimedia Commons user mattes, http://en.wikipedia.org/wiki/File:VTBS-luggage_screening.JPG

What is security?

Security Goals

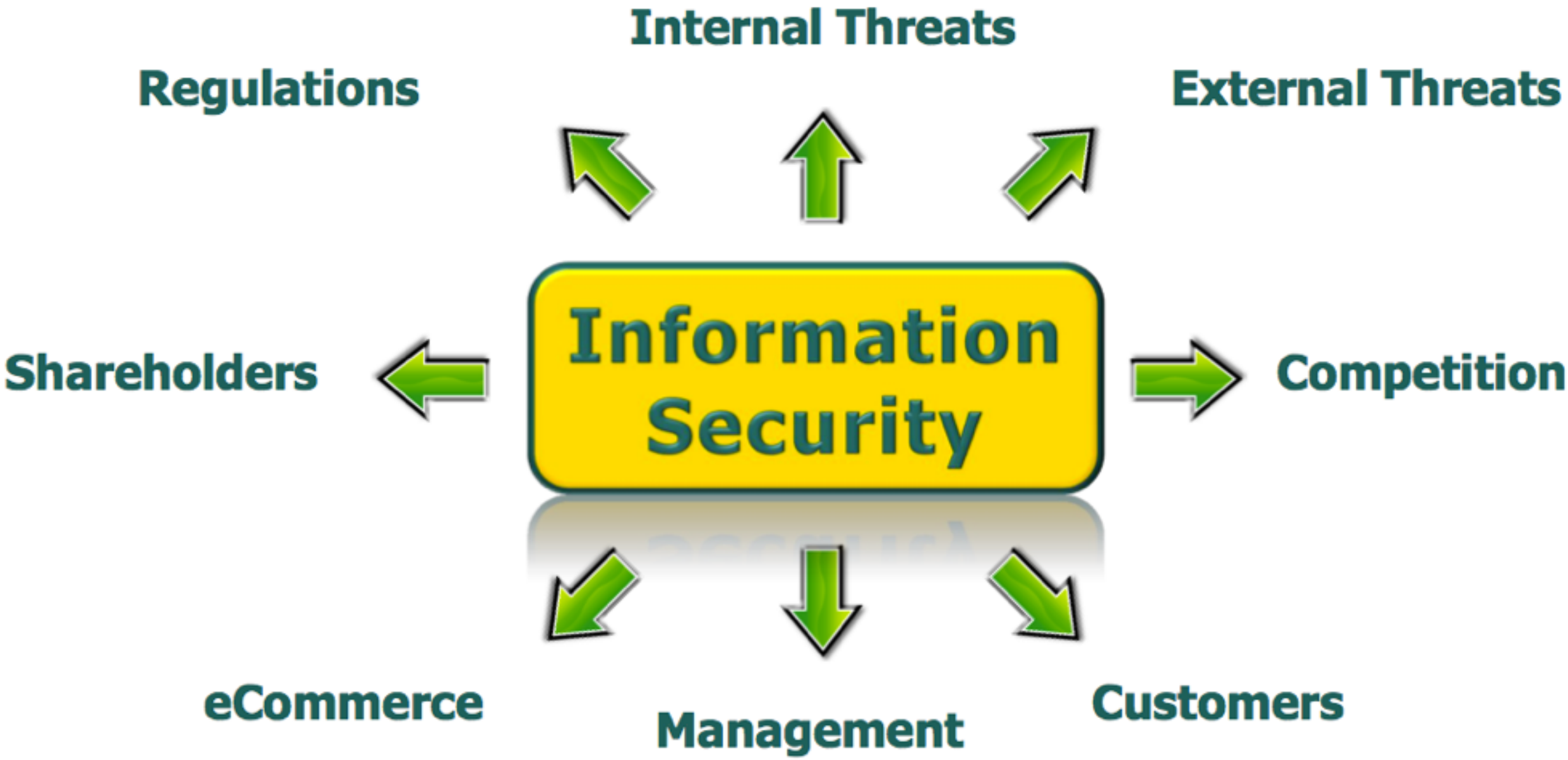
- C (Confidentiality)
- I (Integrity)
- A (Availability)

CIA
Security

Security Mechanisms

- Authentication
- Access Control
- Encryption
- Signatures

Information Security Today



Security Framework

Organizational Security Policy

Statement by top-level management that security is important to the organization and activities pursuant to a secure state will be recognized, supported, and funded

Functional Policies in Support of Organizational Policy

(these are some examples)

Acceptable Use	Anti-virus	Interconnection
Email Use	Firewall	Host Security
Wireless Use	Extranet	Other Policies

Supporting Mechanisms

Standards
define specific products and mechanisms to be used to support policy

Procedures
define actions to implement standards and baselines

Baselines
define minimum required parameters to achieve a consistent security level

Guidelines
define recommended (yet not required) actions

- Provides Management's Goals and Objectives in writing
- Document Compliance
- Create Security Culture

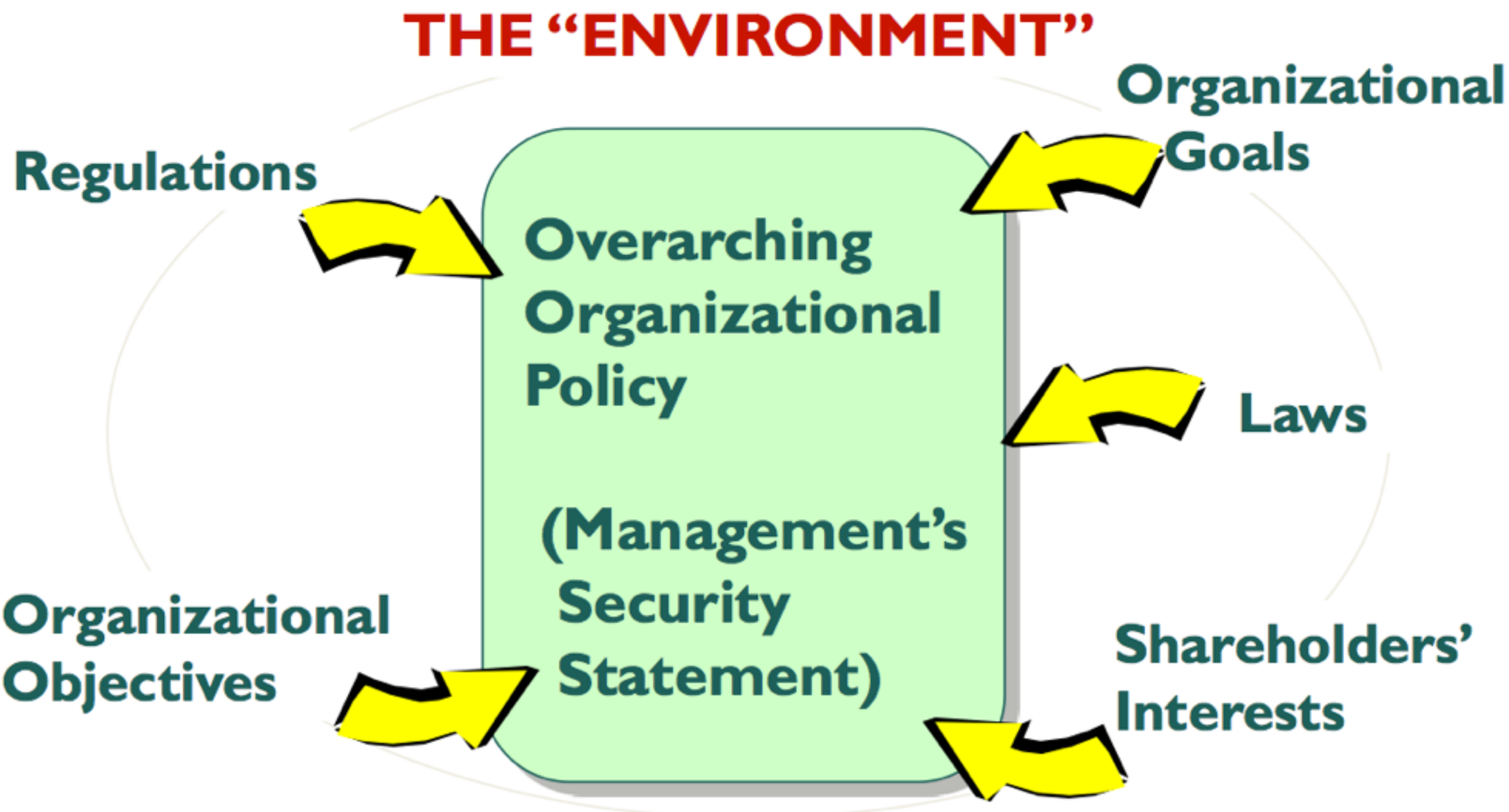
Management's Security Policy

- Provides Management's Goals and Objectives in writing
- Document Compliance
- Create Security Culture

Management's Security Policy

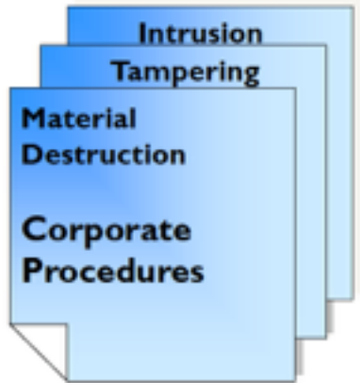
"Security is essential to this company and its future"

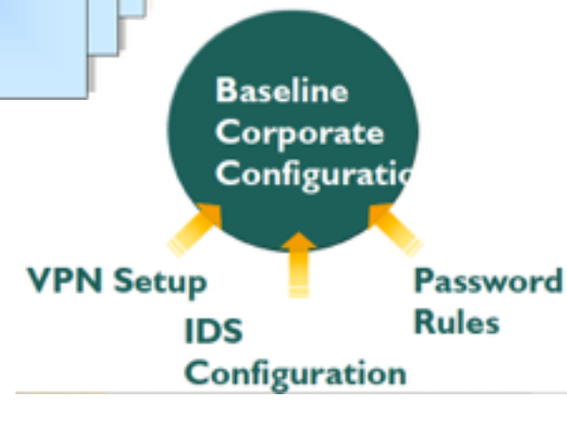
Policy Overview

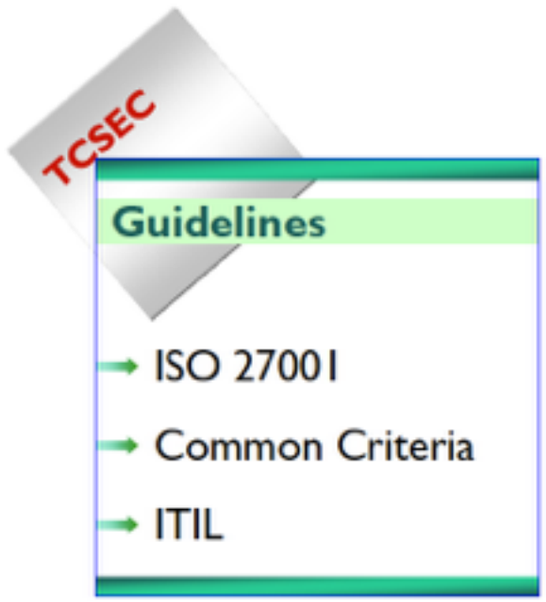


Terminologies

- Procedures
  - Required step-by-step actions
- Baselines
  - Establish consistent implementation of security mechanism
  - Usually platform unique
- Guidelines
  - Recommendations for security product implementations, procurement & planning







PDCA

- New Organization Chart
- Risk Assessment
- Network Design
- Floor plan

Plan

Do

- Policy and Standards
- Countermeasures
- Training Plan

ACT

Check

- Implement new Policies and Standards
- Implement new countermeasures

- Security Audit Plan
- Audit procedure

What is Risk?

- The probability that a particular threat will exploit a particular vulnerability.
- Need to systematically understand risks to a system and decide how to control them.

Pic source : http://www.fiduciarytechnologiesinc.com/files/risk2.jpg

The Elements of Risk

Asset	What we are trying to protect
Vulnerabilities	The weaknesses or faults in our system, processes, awareness or monitoring that could allow an attack to be successful
Threats	The enemy - The forces that may exploit a vulnerability (threat/vulnerability pairing) leading to a successful attack

Risk

Threats

X

Vulnerabilities

Loss , Damage

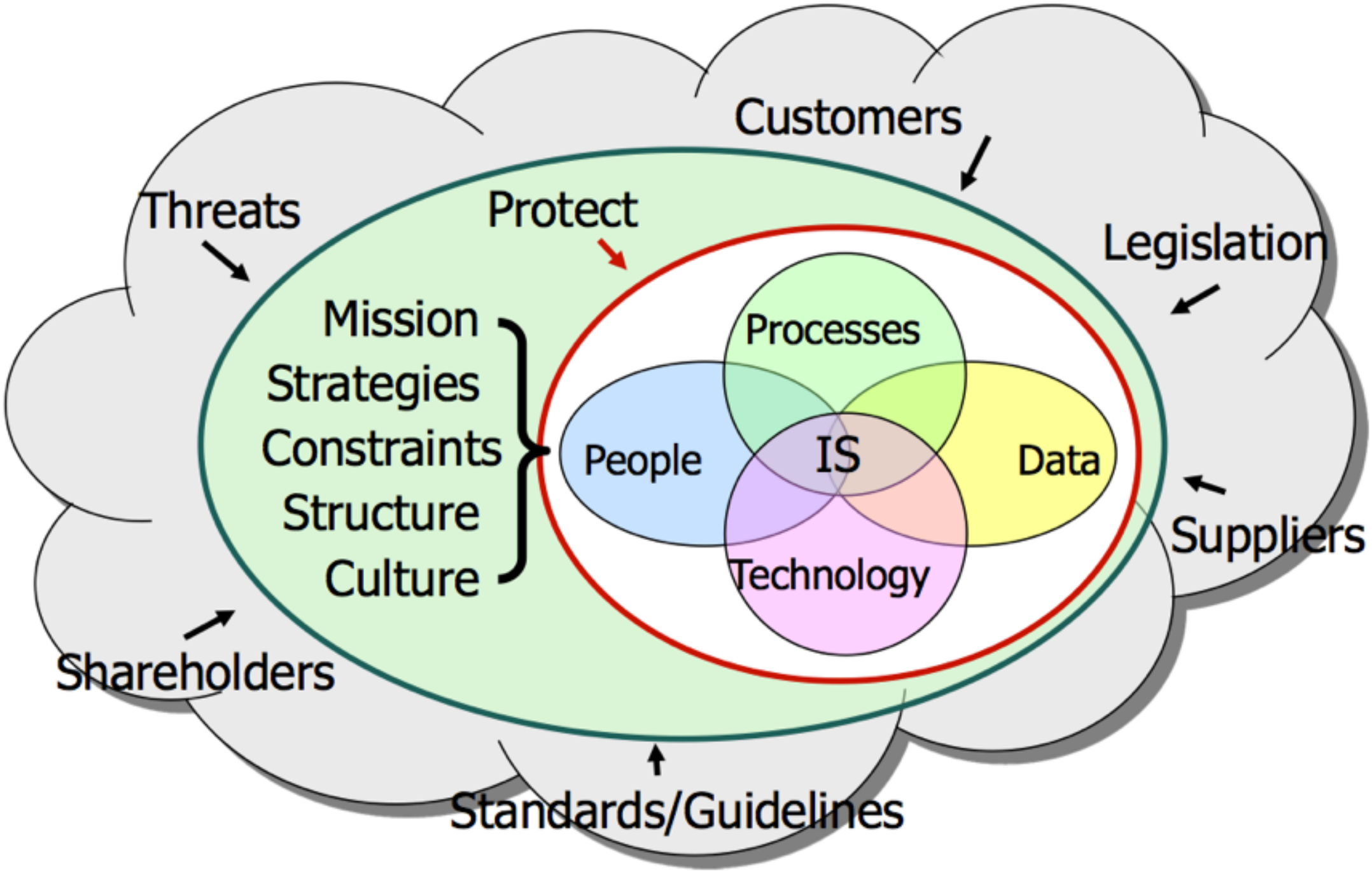
Risks

- Physical damage
- Human interaction
- Equipment malfunction
- Inside and outside attacks
- Data threats
- Application error

Common Vulnerabilities & Attacks

- Vulnerabilities
  - Network: Protocol manipulation, service misuse, plaintext data
  - Program: Buffer Overflow, Format String Attack
  - Operating System: Unpatched service
  - Process/ Implementation: Weak/ sharing of password
- Attacks
  - Network: Sniffing, Denial of service
  - Program/OS: Malicious code, SQL injection, XSS
  - Social engineering attack

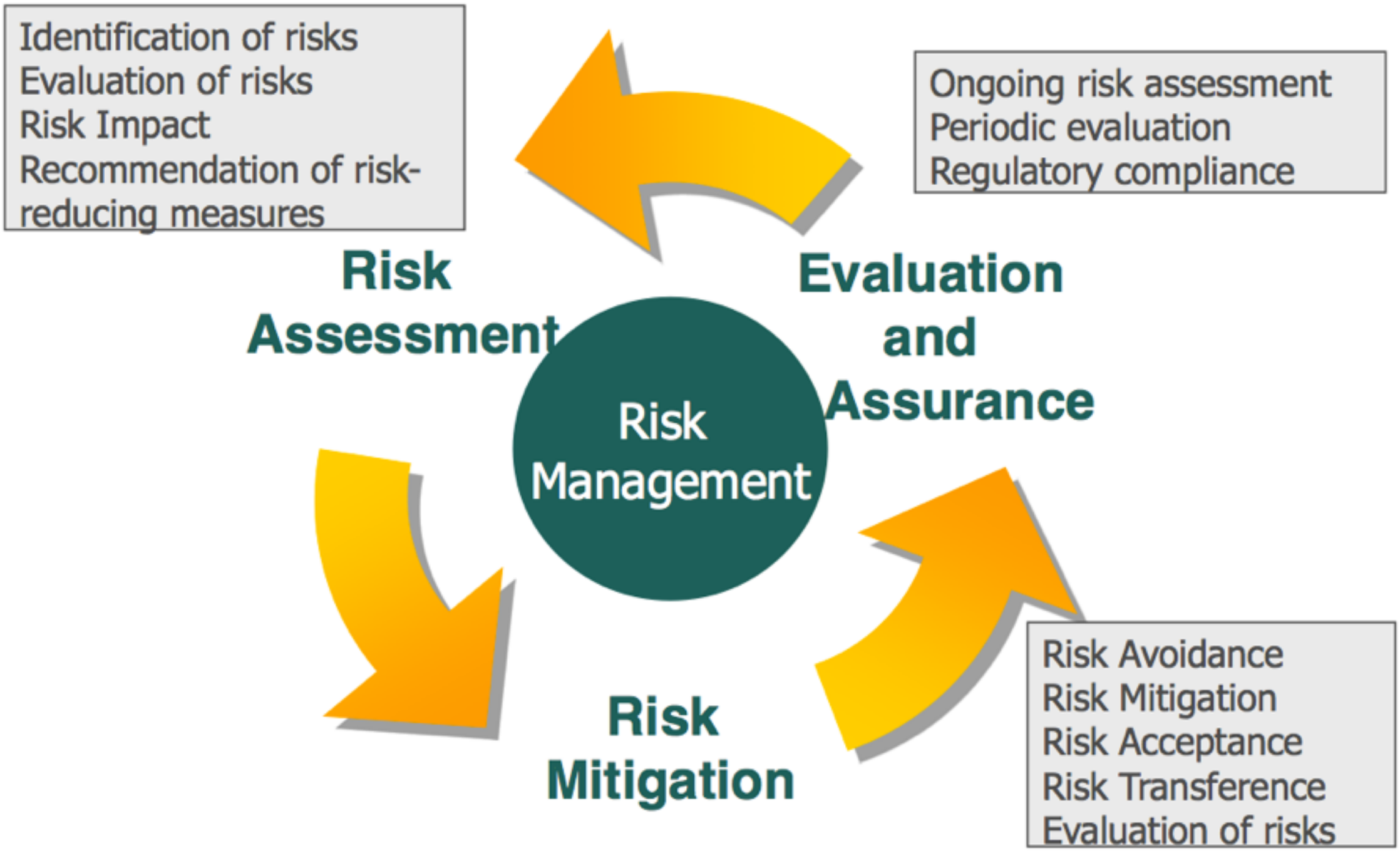
Risk, Response & Recovery



What is Risk Analysis?

- The process of identifying, assessing, and reducing risks to an acceptable level
  - Defines and controls threats and vulnerabilities
  - Implements risk reduction measures
- An analytic discipline with three parts:
  - Risk assessment: determine what the risks are
  - Risk management: evaluating alternatives for mitigating the risk
  - Risk communication: presenting this material in an understandable way to decision makers and/or the public

The Risk Equation



Why Risk Analysis?

- Security risks start when the power is turned-on. At that point, security risks commence. The only way to deal with those security risks is via risk management
- Risks can be identified & reduced, but never eliminated
- The purpose of Risk Analysis is to identify potential problems
  - Before they occur
  - So that risk-handling activities (controls and countermeasures) may be planned and invoked as needed
  - On a continuous basis across the life of the product, system, or project

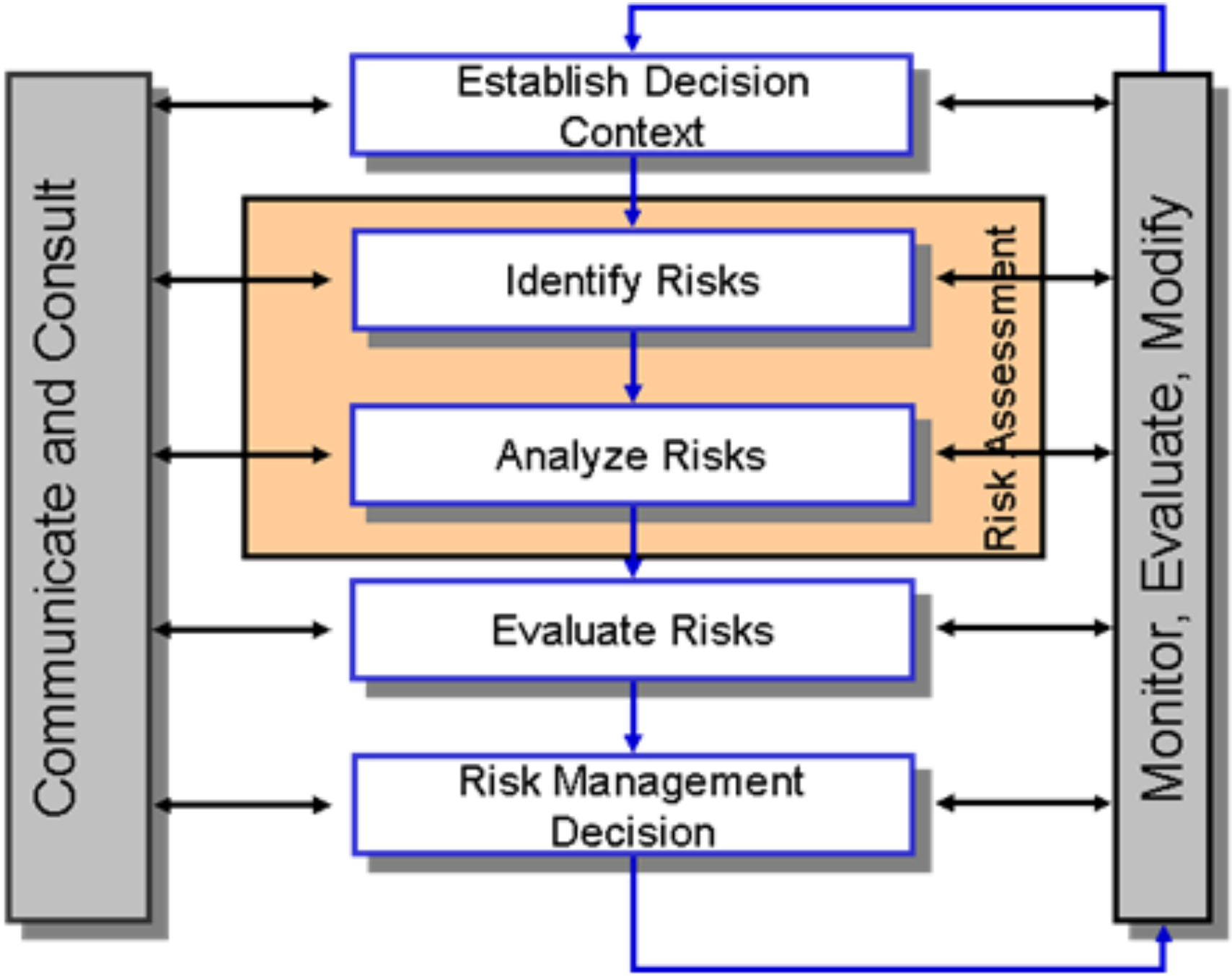
Benefits of Risk Analysis

- Assurance that greatest risks have been identified and addressed
- Increased understanding of risks
- Mechanism for reaching consensus
- Support for needed controls
- Means for communicating results

Key Points

- Key Elements of Risk Analysis
  - Assets, Threats, Vulnerabilities, and Controls
- Most security risk analysis uses qualitative analysis
- Not a scientific process
  - Companies will develop their own procedure
  - Still a good framework for better understanding of system security

Risk Analysis Steps



http://www.corpsnedmanuals.us/DeepDraftNavigation/DDNIncludes/Images/DDNFig2_2RskInfmdDecMkg.png

Risk Management Measurement

Risk Management identifies and prioritizes risks

(Threats, Vulnerability, & Asset Value)

→ TOTAL RISK

Mitigating controls reduce risk:

Total Risk – Mitigating Controls

→ RESIDUAL RISK

- **Residual risk should be set to an acceptable level**

Approaches to Risk Analysis

- Quantitative vs Qualitative Risk Analysis

Quantitative	Numerical Based Data (Hard Data)	Financial data Objective
Qualitative	Scenario Based Data (Soft Data)	Scenario-Oriented Understandability Subjective

- Most organizations will use a hybrid of both approaches to risk assessment.

Risk Example by Asset types

- Hardware
- Software
- Information
- Personnel (People)
- Service
- Location

Hardware

- Asset : Web server
- Threats
  - Hardware failure
- Vulnerabilities
  - Lack of system monitoring
  - Lack of maintenance process
- Controls
  - Monitoring system use (A.10.10.2)
  - Maintenance contract expanded

Software

- Asset : Windows 8
- Threats
  - Use of Pirated Software
- Vulnerabilities
  - Lack of policy restricting staff to use licensed software
  - Lack of user awareness
- Controls
  - Acceptable use of assets
  - Establish formal disciplinary process

Information

- Asset : Confidential files
- Threats
  - Disclosure of confidential information
- Vulnerabilities
  - Lack of information & document classification and handling procedure
  - Lack of Physical security
  - Lack of User awareness
- Controls
  - Establish or implement procedures in information handling
  - Define rules for working in secure areas
  - Information Security Education and Training

Personnel

- Asset : Clerk
- Threats
  - Operational Staff or User Errors
- Vulnerabilities
  - Lack of efficient and effective configuration change control
  - Lack of technical skill
  - Lack of User awareness
- Controls
  - Establish change control management
  - Information Security Education and Training

Personnel (2)

- Asset : Clerk
- Threats
  - Resign
- Vulnerabilities
  - Lack of cross-function / backup staff
  - Poor employee relationship management
- Controls
  - Provide cross-functional training for key job function
  - Management should provide the resources needed

Services

- Asset : Network system
- Threats
  - Failure of communication services
- Vulnerabilities
  - Lack of redundancy
- Controls
  - Arrange backup internet service
  - Use redundant Internet service (two ISPs)

Location

- Asset : Head office building
- Threats
  - Sabotage
- Vulnerabilities
  - Lack of Physical Security
  - Lack of Change Management Controls
- Controls
  - Implement environment threats protection
  - Establish formal physical entry controls
  - Establish change control management

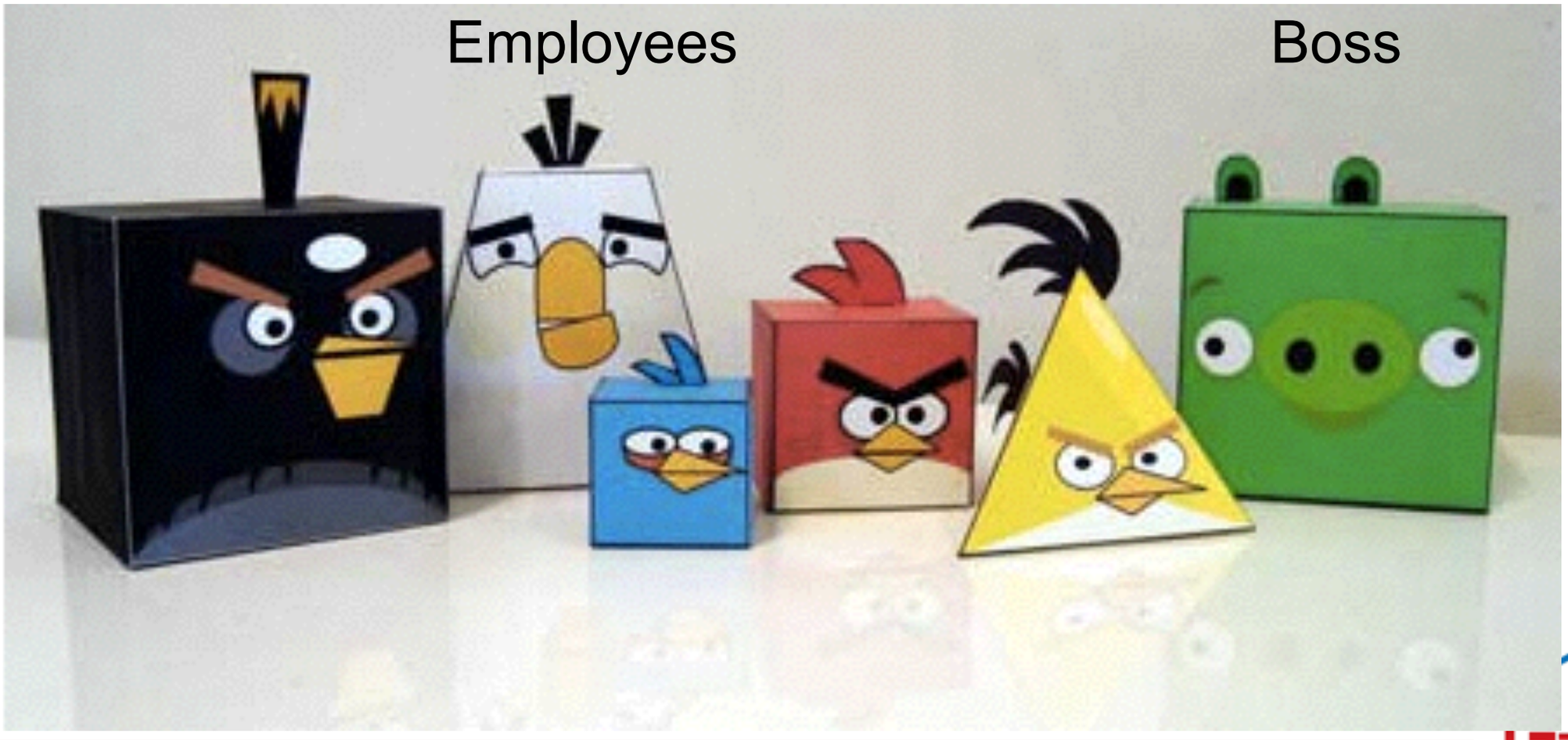
Group Activity#1 - Risk assessment

- Separate into 3 groups
  - IT Support
  - Server/Network Administrator
  - Software/Web Development
- Define your assets in your organization
- Try to think about threats and countermeasure which is possibly related to your assets above
- and present
- 30 minutes

Risk Management

When Risks are happened ....

- What should we do, if we are management level?
- In case of Facebook and Youtube are risks



Risk Management

AVOID

ACCEPT

REDUCE

TRANSFER/SHARE

Key to success for IT security implementation

- Supported by CEO or management level
- Implement most suitable IT security tools (both quality and budget)
- Every departments are involved to do risk assessment/analysis
- All of employees have awareness

Threat Landscapes

- Exploitation
- Web application hacking
- Botnet
- Malware/ Ransomeware
- Phishing/ Spear Phishing
- Port scanning
- Brute force (Login attempts)

- anything else?

Exploitations

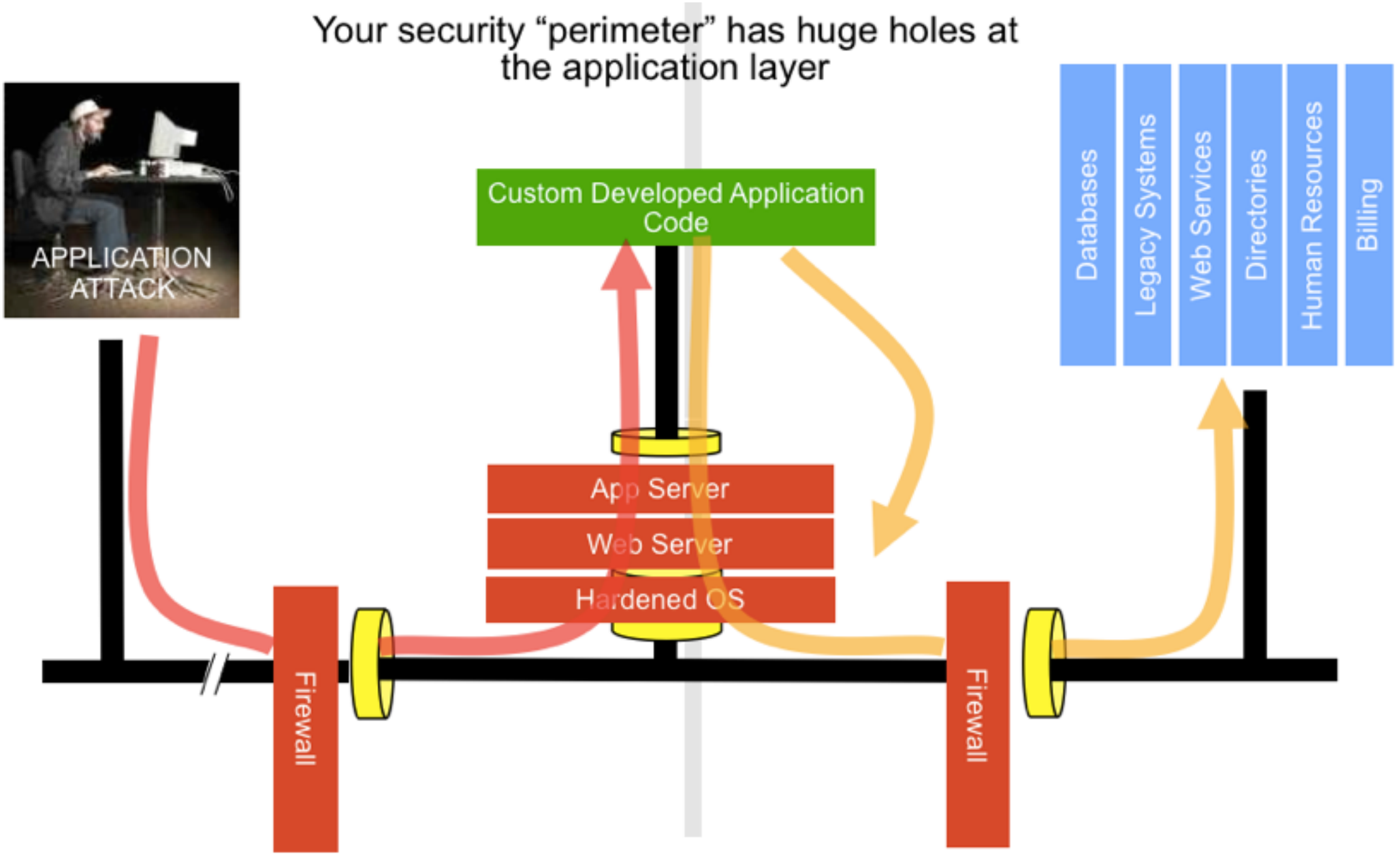
- Target on 0-day vulnerabilities
- Heartbleed
- ShellShock

```
root@ubuntu:~# env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
```

Web Attacking

- Web Defacement
- Malicious script spreading
- Phishing
- Database and Credential stolen

Why we need web application security?



You can’t use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks

Network Security is not enough

- Network Security Mostly Ignores the Contents of HTTP Traffic, such as....
  - Firewalls, SSL, Intrusion Detection Systems
  - Operating System Hardening, Database Hardening
- Need to secure web application (Not Network Security)
  - Securing the "custom code" that drives a web application
  - Securing libraries
  - Securing backend systems
  - Securing web and application servers
- **Cloud Computing is coming**, the infrastructure is secured by the provider but we are still need to secure our application.

OWASP

- Open Web Application Security Project
- http://www.owasp.org
- Open group focused on understanding and improving the security of web applications and web services!
- Hundreds of volunteer experts from around the world

OWASP
The Open Web Application Security Project
http://www.owasp.org

OWASP
The Open Web Application Security Project

Navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Press
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists
- About OWASP
- Membership

Reference

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Controls

Main Page

Welcome to OWASP
the free and open application security community

- OWASP Summit 2011
- Top Ten
- WebScarab
- ESAPI
- ASVS
- AntiSamy

About • Searching • Editing • New Article • OWASP Categories

The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

You'll find everything **about OWASP** here on our wiki and current information

Special

Quick Reference

Election of Officers Upc

Community Forums - C

Contact OWASP Staff -

Industry Citations - Cli

Podcast - Listen Now

Blog - Click Here

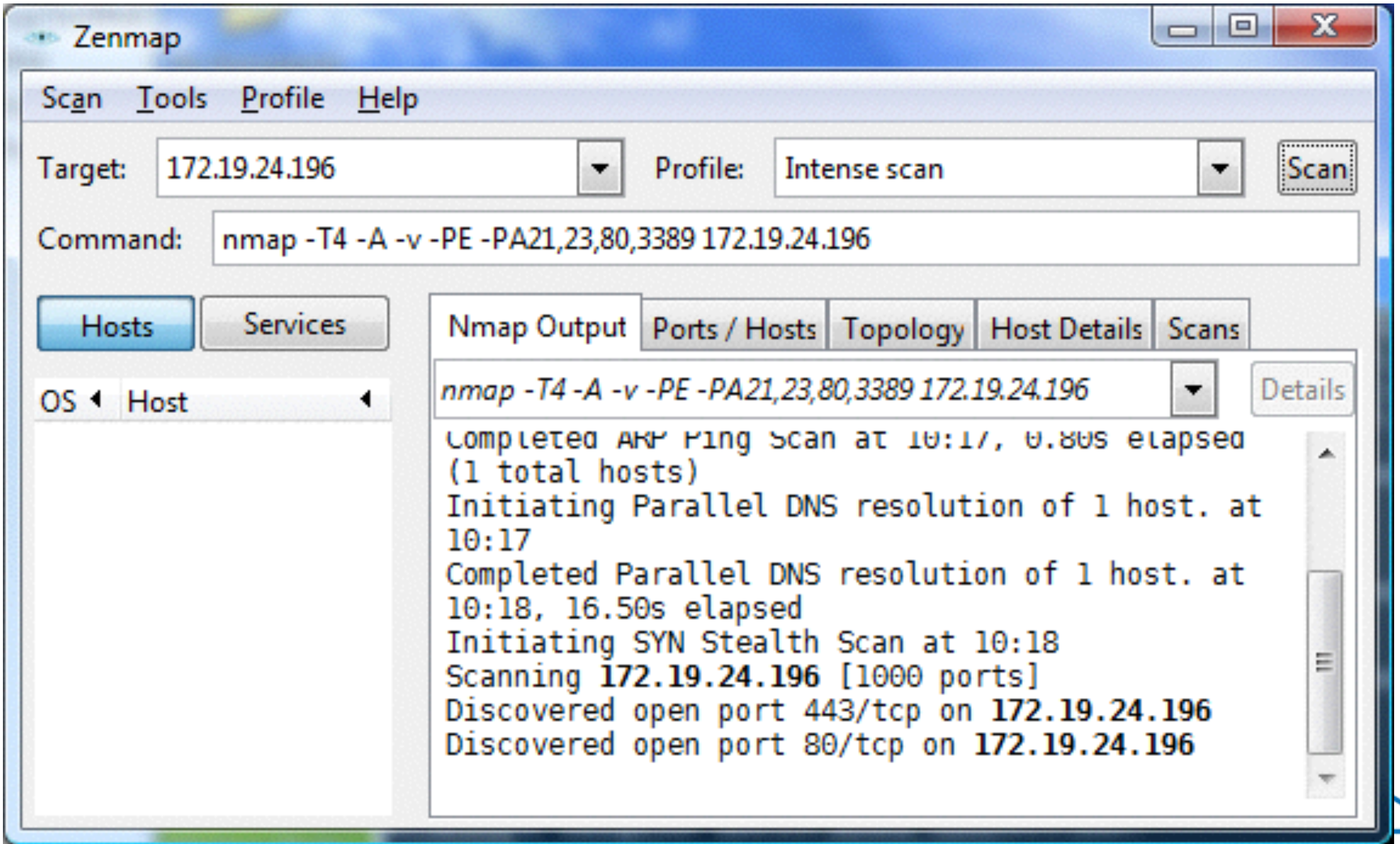
EGA e-Government Agency

G-CERT by EGA

Probe Scan

- Port scan - To check which ports are opened and guess what services are running.
  - nmap
- Vulnerability scan - To check which services or software are vulnerable
  - Nessus
- Login Attempts - To check for weak password accounts
  - Password attack (brute force, dictionary, rainbow)
- Malware Attack (Port + Vulnerability + Login)

nmap (Windows)



SSH login attempts

test.pcap – Wireshark

nalyze Statistics Telephony Tools Help

Expression... Clear Apply

Source	Destination	Protocol	Info
136.206.1.49	192.168.1.34	SSH	Encrypted request packet len=144
192.168.1.34	136.206.1.49	TCP	ssh > 44481 [ACK] Seq=1886 Ack=1369 Win=32929 Len=0 TSV=841350482 TS
192.168.1.34	136.206.1.49	SSH	Encrypted response packet len=80
136.206.1.49	192.168.1.34	TCP	44481 > ssh [ACK] Seq=1369 Ack=1966 Win=83 Len=0 TSV=3064621367 TSER
136.206.1.49	192.168.1.34	SSH	Encrypted request packet len=144
192.168.1.34	136.206.1.49	TCP	ssh > 44481 [ACK] Seq=1966 Ack=1513 Win=32929 Len=0 TSV=841350498 TS
192.168.1.34	136.206.1.49	SSH	Encrypted response packet len=80
136.206.1.49	192.168.1.34	TCP	44481 > ssh [ACK] Seq=1513 Ack=2046 Win=83 Len=0 TSV=3064622899 TSER
136.206.1.49	192.168.1.34	SSH	Encrypted request packet len=144
192.168.1.34	136.206.1.49	TCP	ssh > 44481 [ACK] Seq=2046 Ack=1657 Win=32929 Len=0 TSV=841350522 TS
192.168.1.34	136.206.1.49	SSH	Encrypted response packet len=80
136.206.1.49	192.168.1.34	TCP	44481 > ssh [ACK] Seq=1657 Ack=2126 Win=83 Len=0 TSV=3064625357 TSER
136.206.1.49	192.168.1.34	TCP	44481 > ssh [FIN, ACK] Seq=1657 Ack=2126 Win=83 Len=0 TSV=3064625358
192.168.1.34	136.206.1.49	TCP	ssh > 44481 [ACK] Seq=2126 Ack=1658 Win=32965 Len=0 TSV=841350525 TS
192.168.1.34	136.206.1.49	TCP	ssh > 44481 [FIN, ACK] Seq=2126 Ack=1658 Win=32965 Len=0 TSV=8413505
136.206.1.49	192.168.1.34	TCP	44481 > ssh [ACK] Seq=1658 Ack=2127 Win=83 Len=0 TSV=3064625663 TSER

bytes captured)

e:0e (00:a0:c5:fd:9e:0e), Dst: Apple_ad:ec:5a (f8:1e:df:ad:ec:5a)

.1.49 (136.206.1.49), Dst: 192.168.1.34 (192.168.1.34)

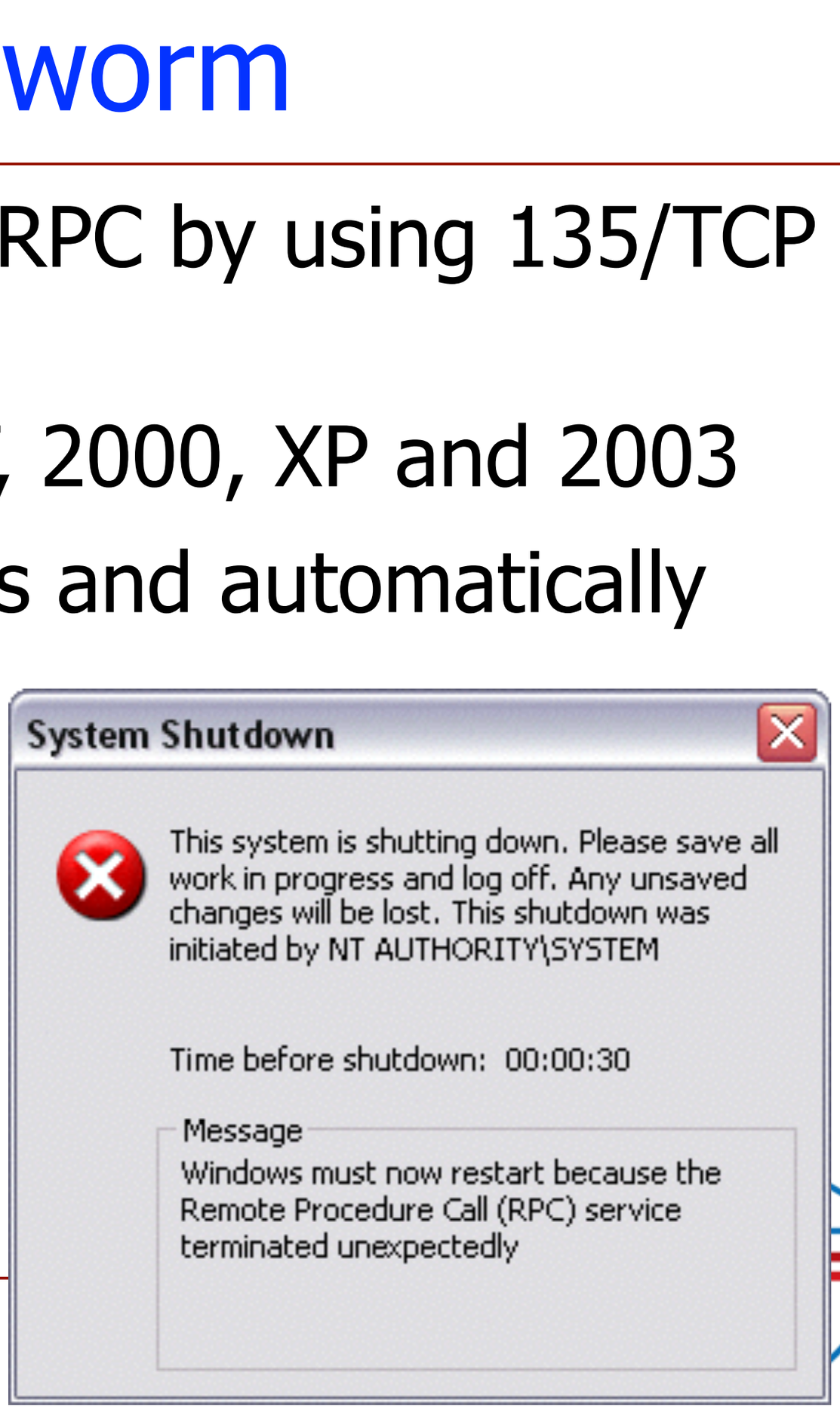
Src Port: 44481 (44481), Dst Port: ssh (22), Seq: 1658, Ack: 2127, Len: 0

```
fd 9e 0e 08 00 45 00   .....Z.. ......E.
97 88 ce 01 31 c0 a8   .4.c@.6. *....1..
5a 05 62 b0 11 80 10   ."...... .Z.b....
```

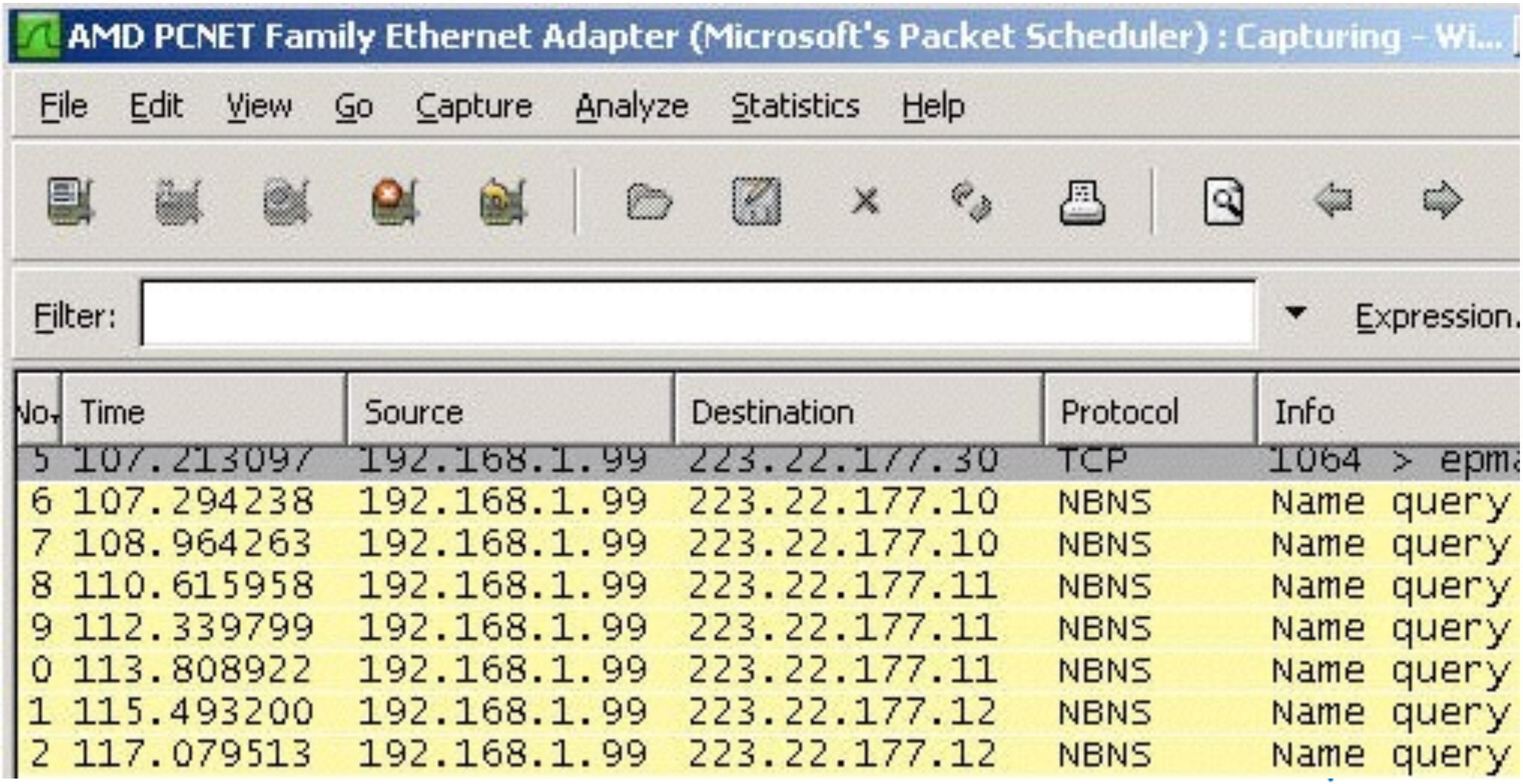
Blaster worm

- Analyze Attack DCOM RPC by using 135/TCP and 137/UDP
- Effect for Windows NT, 2000, XP and 2003
- Countdown 30 seconds and automatically restart

Jeffrey Lee Parson, 19
Blaster worm writer



Blaster's traffic

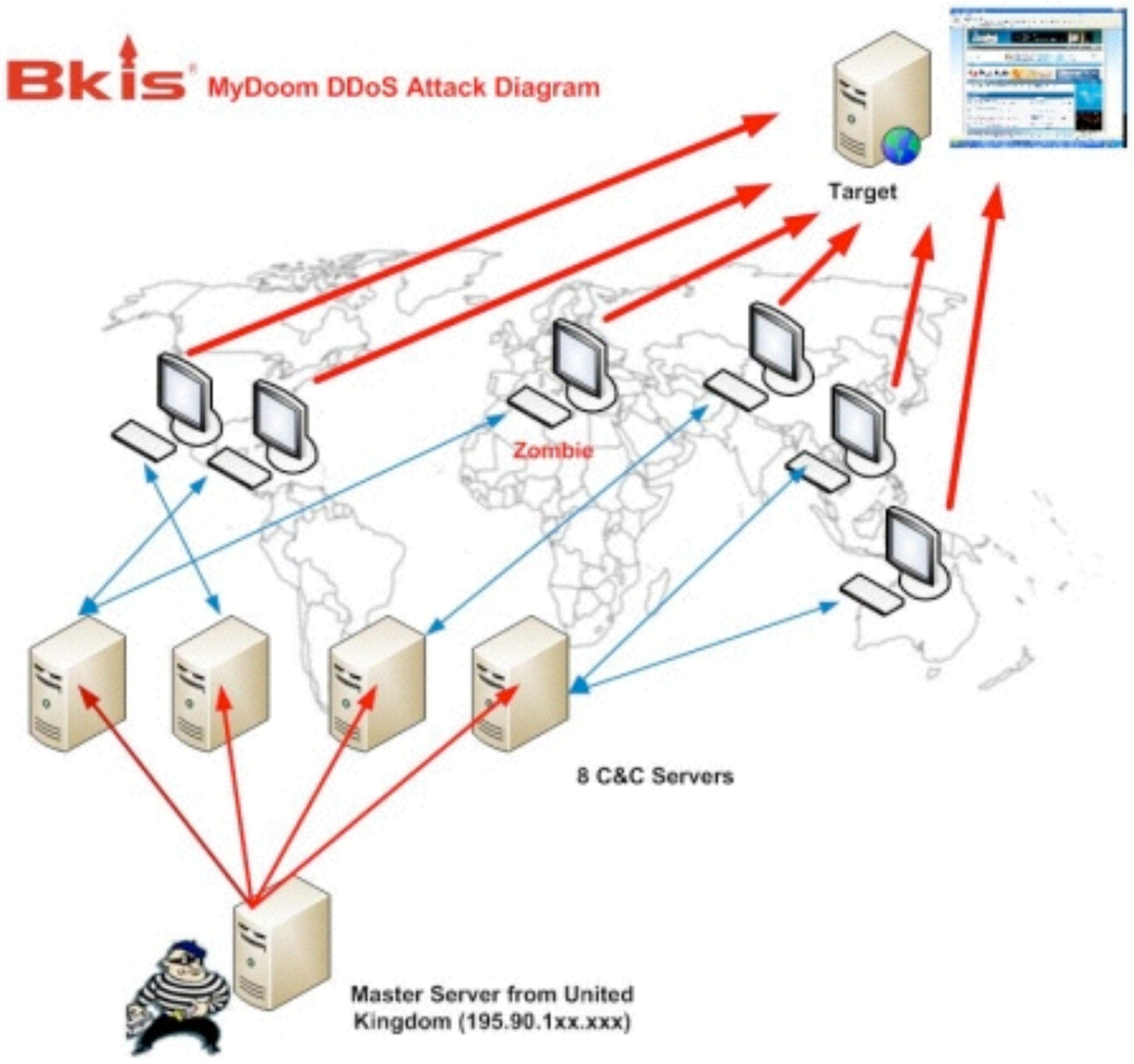


Ransomware

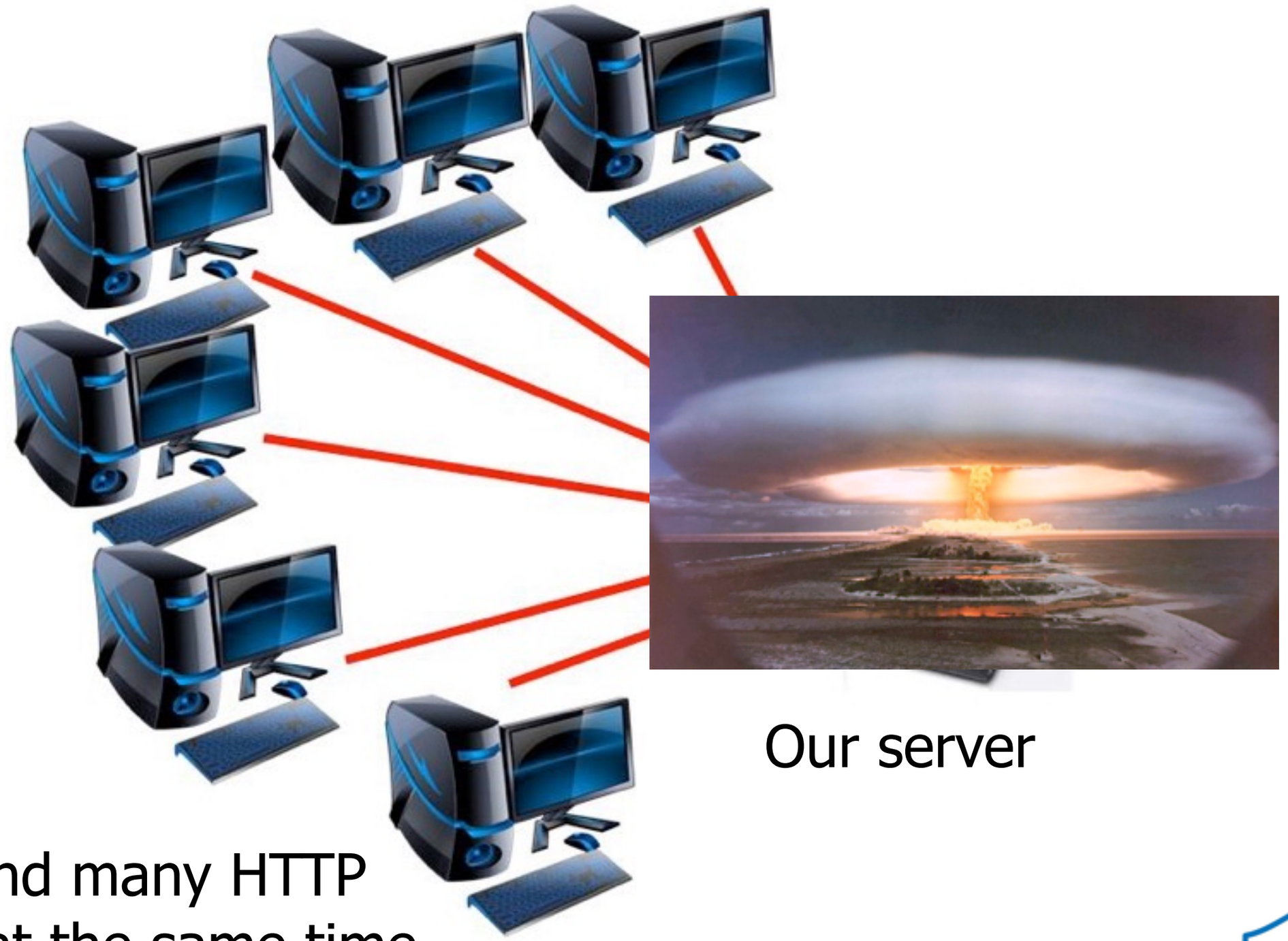
- Several companies were infected
- All important and document files are encrypted by RSA-4096 (No way to decrypt)
- Need much better backup process

CryptoLocker

Botnet & DDoS


Bkis
MyDoom DDoS Attack Diagram
Target
Zombie
8 C&C Servers
Master Server from United Kingdom (195.90.1xx.xxx)

Distributed Denial of Service (DDoS) - Flooding



Our server

Botnet send many HTTP requests at the same time

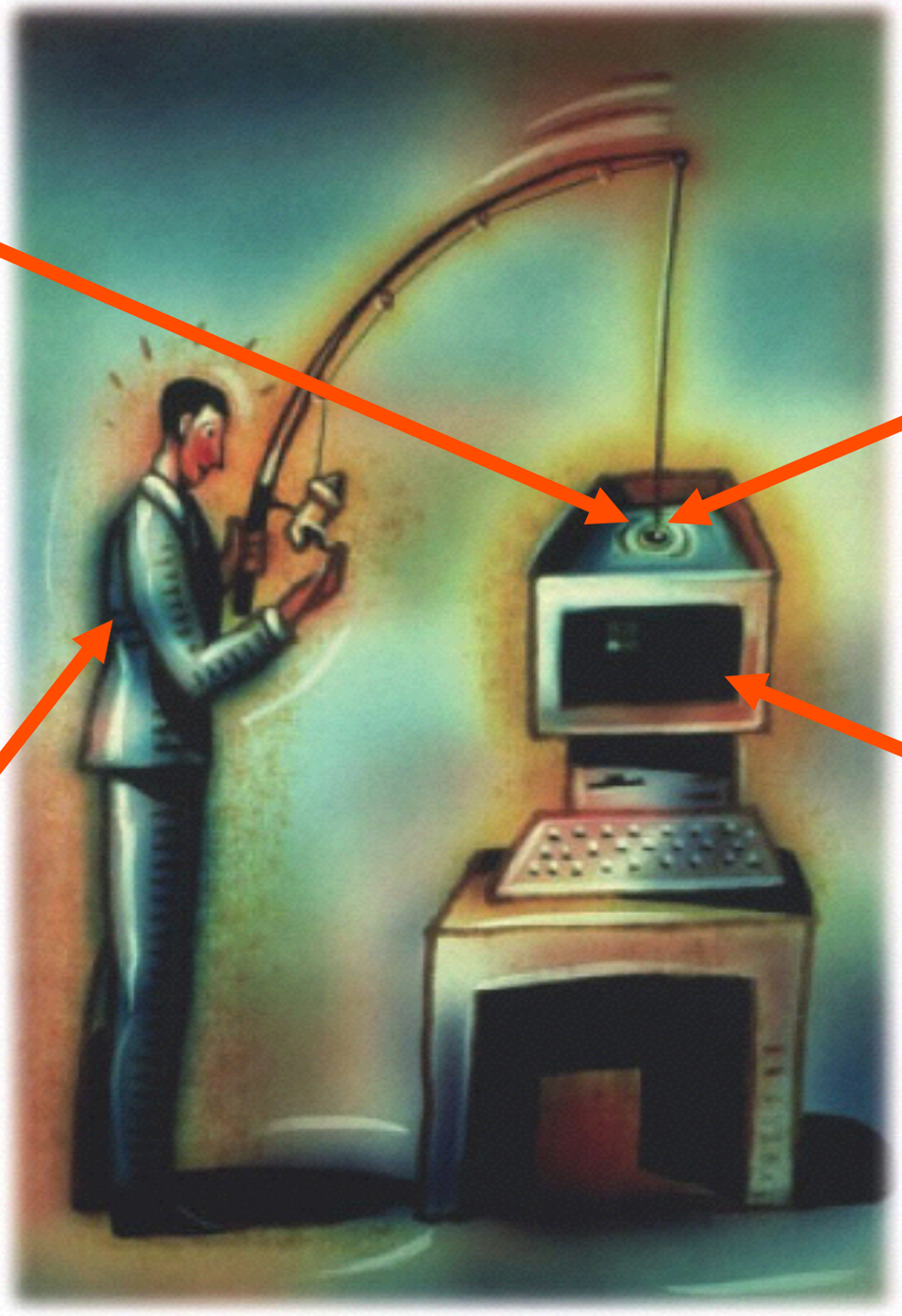
Over consuming

Your server is like the donkey, and no, it’s not the donkey’s fault.

Phishing

Spam

(Food)



Faked website

(Hook)

Phisher

(Fisher)

Victim

(Fish)

Spear Phishing

http://www.terrapapers.com/wp-content/uploads/2013/10/Spear-phishing-1.png

Example

Gmail by Google

Dale Peterson <peterson@digitalbond.com>

(no subject)

1 message

Dale Peterson <dale.peterson111@yahoo.com> Thu, Jun 7, 2012 at 7:48 AM
Reply-To: Dale Peterson <dale.peterson111@yahoo.com>
To: "rvpasupuleti@yahoo.com" <rvpasupuleti@yahoo.com>

Dear All:
Field devices essential for the monitoring and control in DCS and SCADA systems are increasingly being deployed with Ethernet cards to connect these devices to local and wide area IP networks. Many of the Ethernet cards have their own CPU, memory, operating system and applications. Field device vendors are also providing the capability to upgrade or replace the firmware in these Ethernet cards. Unfortunately in most cases there is no effective security on the firmware upload to the field device Ethernet cards.
Details are available at: Leveraging_Ethernet_Card_Vulnerabilities_in_Field_Devices.pdf
Download it and have a look.
Regards,
Peterson

Incident Handling

Overview - Typical IT Security

But.....


More Security Doesn't Make You More Secure
Better Management Does.

Controls will be bypassed

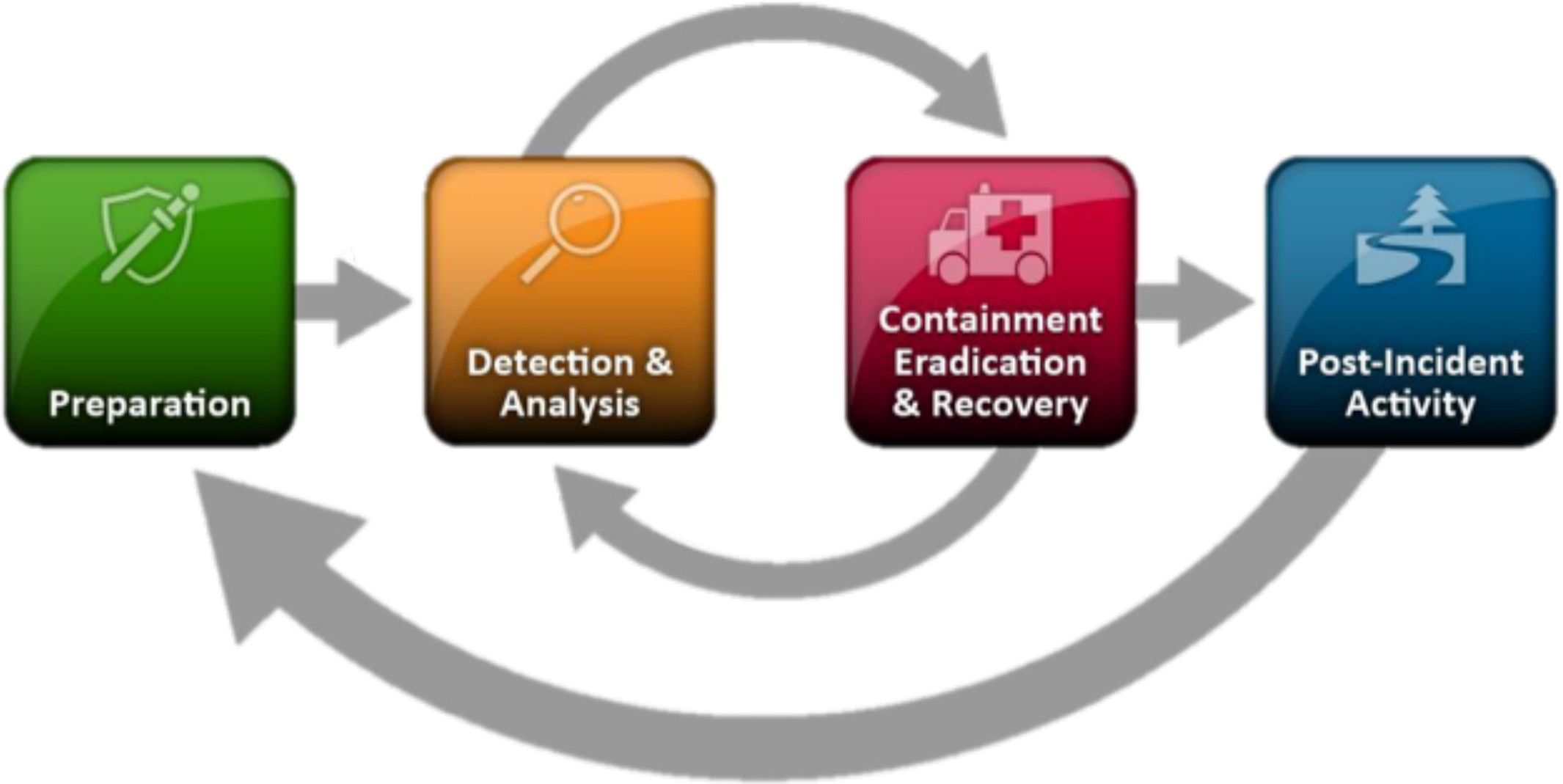
Traditional Incident Response

- Adhoc & Unplanned
- Deal with it as it happens
- Prolonged Recovery Times
- Damage to Company
- Lack of Metrics
- Legal Issues
- Bad Guys/Gals Getting Away

You In Line of Fire

Processes

- Incident Response plan



IR Plan - Preparation

- Build the secured infrastructure
- Security policy
- Setup the monitoring system
- Prepare IR Team and process

IR Plan - Detect & Analysis

- Setup the monitoring system
- Read logs
- Maybe someone reports
- Analysis when something's happened

IR Plan - Response, Eradication and Recovery

- Find the attackers and how
- Remove or correct the system
- Operate the system again

IR Plan - Post incident activities

- Study from the attacks
- Prepare the protections
- Keep record

Thank you