menog
MIDDLE EAST
NETWORK OPERATORS GROUP
A forum for network operators in the Middle East

RIPE NCC

Network Security

MENOG 4/RIPE NCC Regional Meeting, Manama, Bahrain
9 April 2009

Alaa Al-Din (Aladdin) Jawad Kadhem Al-Radhi :
Consultant Engineer and Researcher
Masters CINS "Computer Information Network Security"
DePaul Univeristy Chicago, Illinois USA
alradhi2000@yahoo.ca alaalradhi@hotmail.com
+ 962 796347600

Motto: You can NOT predict when and where things will happen, So you'll have to understand the how!

About Me! Passionate / Advocate of All Internet Works, Advances, Researches, Collaborations, etc

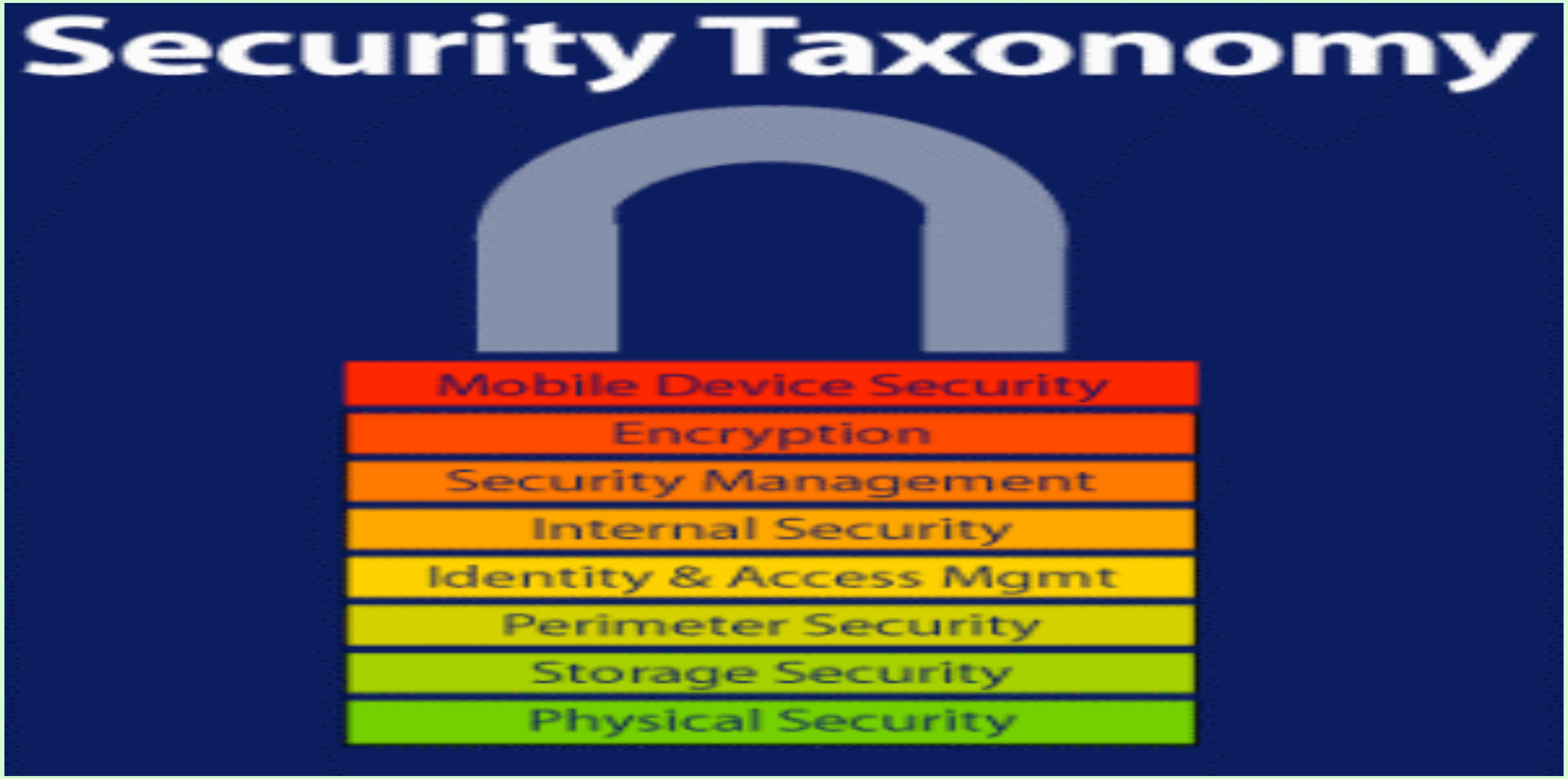
- Advisory Council Member of PIR (Public Interest Registry), www.pir.org
- ICANN “Board of Directors” Nomination Candidate 2009-2011, and Fellow www.icann.org
- AKMS (Arab Knowledge and Management Society) “Board of Trustees” Member, www.akms.org
- ISOC (Internet Society) IGF Ambassador and Global Member www.isoc.org
- ITU Arab Regional Office affiliated Consultant, speaker and presenter www.itu.int
- DIPLO Foundation Internet Governance Fellow www.diplomacy.edu
- DePaul University Security Group, Alumni and International Contact www.depaul.edu
- Member of “Internet 2” www.internet2.edu Middle East Group
- Member of “EUMEDCONNECT 2” www.eumedconnect2.net Middle East Group
- Member of ASIWG “ Arabic Script Internationalized Domain Names Work Group www.arabic-script-domains.org
- Member of AOIR “Association Of Internet Researchers” www.aoir.org
- Fellow of RIPE-NCC & MENOG “ Middle East Network Operators Group” www.ripe.net and www.menog.net
- Information Share Award Winner 2007-2009 & Member of ASIS&T “ American Society for Information Science and Technology” www.asis.org
- Steering Committee Member ACS Arab Computer Society www.arabcomputersociety.org
- Member of EU Communications and Research Association www.ecrea.eu
- Member of IHEOST “Iraq Higher Education Organization for Science & Technology” www.wmin.ac.uk/iraq-he & www.iraqhe.com

Worried Being Always At Risk?!
Then:

- 1st : Know the Basics
- 2nd : Know the Mistakes
- 3rd : Know the Enemy & Threats
- 4th : Start Your Security Roadmap & Learn

1st :

Know The Basics



Bear in Mind:
Enterprise Security is:

- NOT:
  - An ONLY Product that you purchase
  - An ONLY Technology that you use
  - An ONLY Policy that you just agree
  - An ONLY a ONE time Investment
- Having the weakest link: Human Factor!
- Covers your overall enterprise aspects:
  - WHAT: assets? Risks to those assets?
  - HOW: You will do it? Solutions? Other risks may be imposed?
- Conclusion: Security is an ongoing Process = "Technology + Policies + People Good Practices + Training + Awareness" with human factor as the weakest part. A 24X7X365 Process.

Security Basic Terms:

- Threat:
  - Probability of an attack: e.g. transmission of a TCP/IP packet to cause buffer overflow
- Vulnerability:
  - Probability of an exploitable vulnerability: e.g. Buffer overflow
- Consequence: Total Cost of a successful attack

Risk = [Threat x Vulnerability x Consequence], for e.g. System Crash

- Perimeter: Network boundary that include Routers, Firewalls, IDS/IPS, DMZ, etc
- Intrusion Detection System (IDS):
  - Sensor's used to detect/alert on malicious events
- Intrusion Prevention System (IPS):
  - IDS with active components that can stop malicious events automatically
- De-Militarized Zone (DMZ):
  - Area of network between Border Router and Firewall that contains public services.

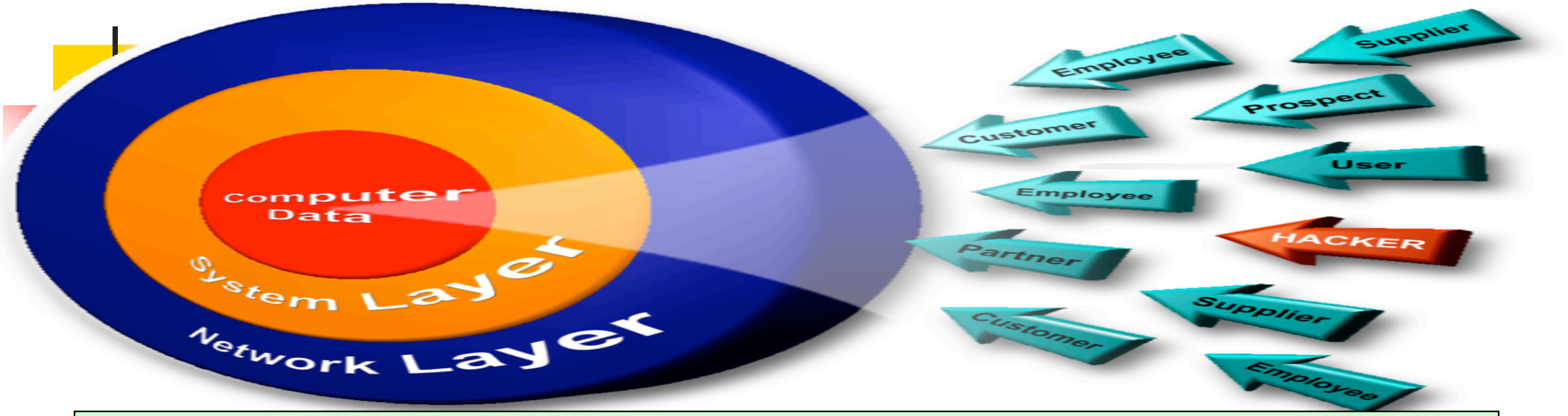
Enterprise Security Thinking Hat:

- Why:
  - Prevent security problems
  - Mitigate security problems: Detect intrusions & Analyze intrusions
  - Recovery: Incidents Reporting's & countermeasures actions!
- How:
  - Prerequisites: Risk and security awareness & Accepted policy
  - Secure Network Design: Multi-layered defense strategy
  - System Design: Strong access control, Strong software security, Accounting and auditing
- Where:
  - Physical : Physical Barriers & Restricted Access to Authorized ONLY
  - Host: IDS Intrusion Detection System & File Integrity Checkers
  - Network: Firewalls, IDS & Vulnerability Scanners
  - Web Application: Search engines, Webmail, shopping carts and portal systems

Enterprise Security Technicalities:

- Defense in Depth: NO single security measure is sufficient! If some layers fails, others can detect. So Multiple layers to detect attacks:
  - Router : 1st line of defense
  - Bastion hosts: Systems visible / available to outside world (e.g. web server)
  - Firewall : 2nd line of defense
  - Secure intranet : Internally available systems
  - IDS/IPS : Distributed Sensors everywhere (depends on vendors)
  - Antivirus / Antimalware: Host machines
- Network Segmentation:
  - Different zones for different functions
  - Contains threats to specific resources
- Perimeter Defense: Protects the borders between network zones
- Network Containment: Limits network to known extent

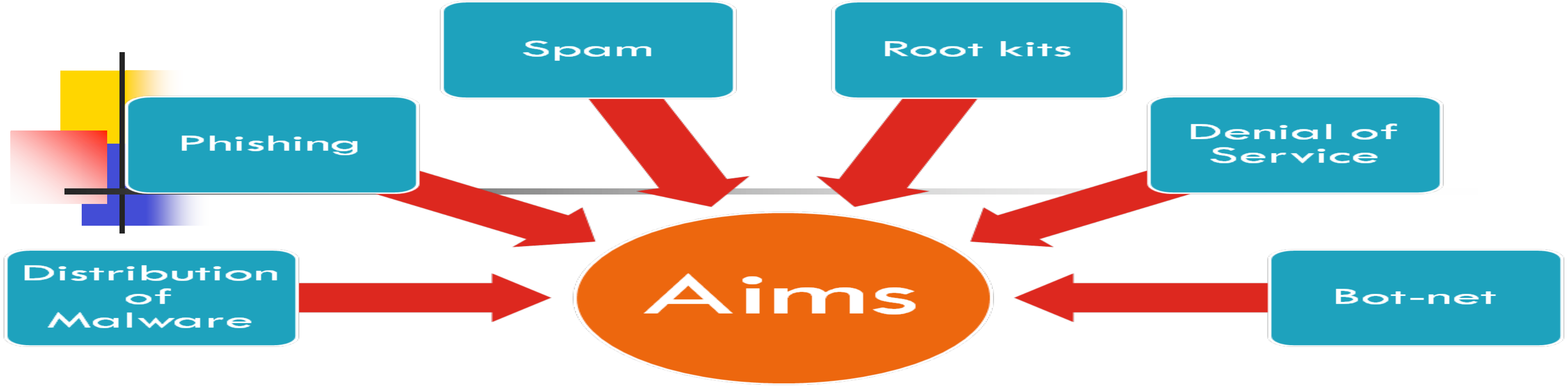
1. So: NOTHING is Secure:



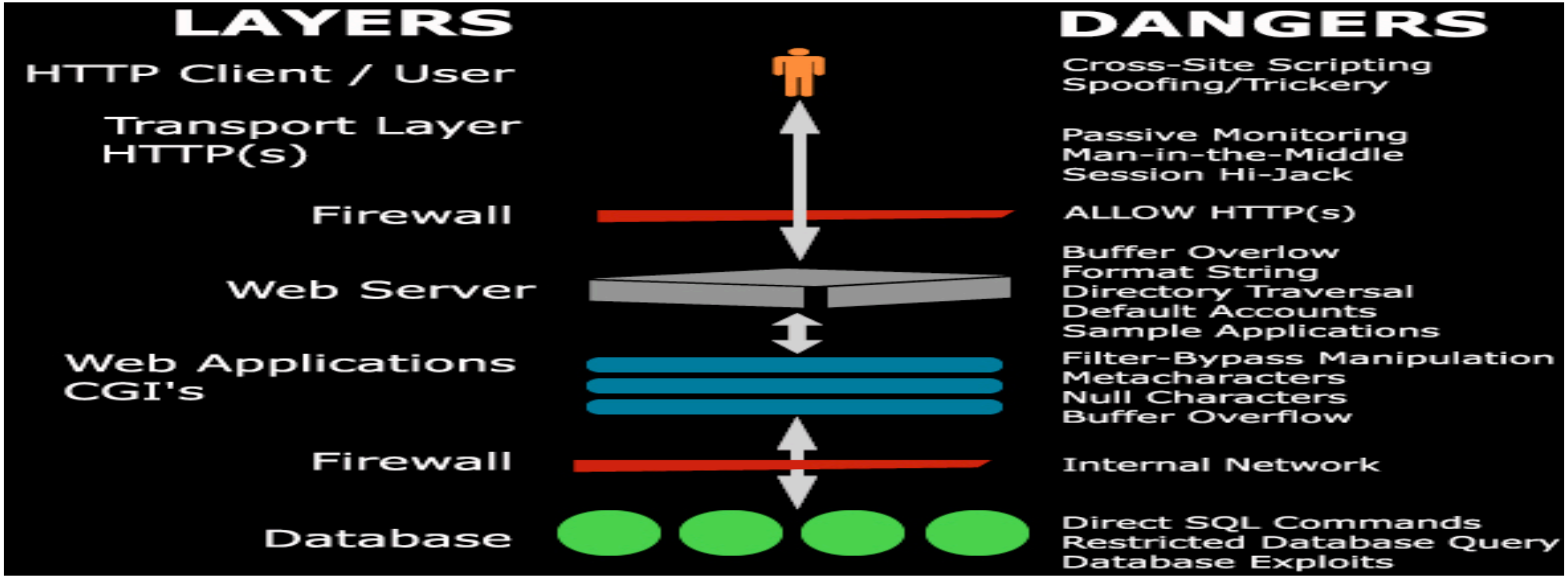
2. And: Different Types of Vulnerabilities:

Client-side Vulnerabilities	• Web Browsers • Email Clients • Media Players
Server-side Vulnerabilities	• Web Applications • Database Software
Security Policy and Personnel	• Phishing/Spear Phishing
Application Abuse	• Instant Messaging • Peer-to-Peer Programs
Zero Day Attacks	• Zero Day attacks

3. Hence: Different Threats:

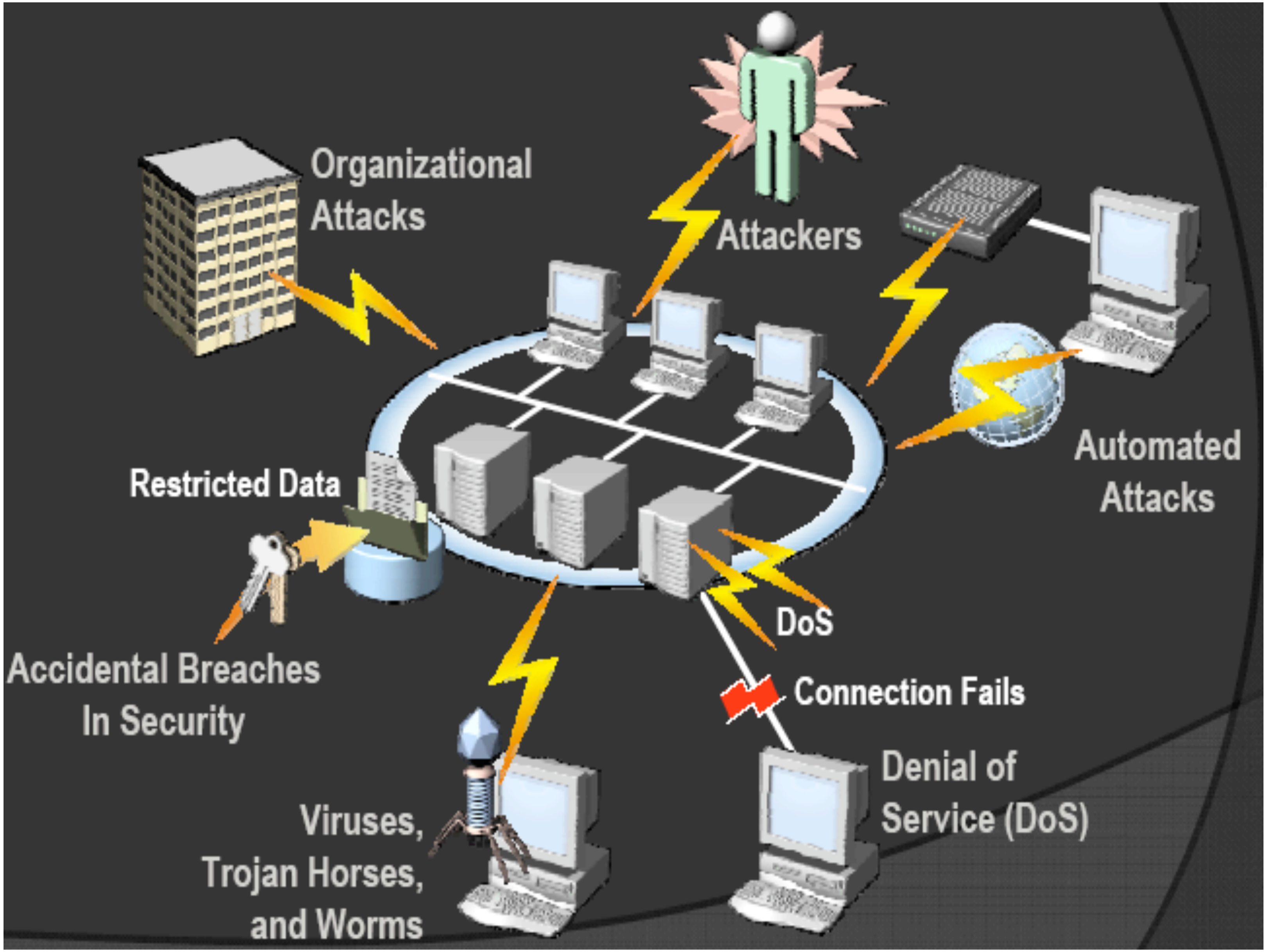


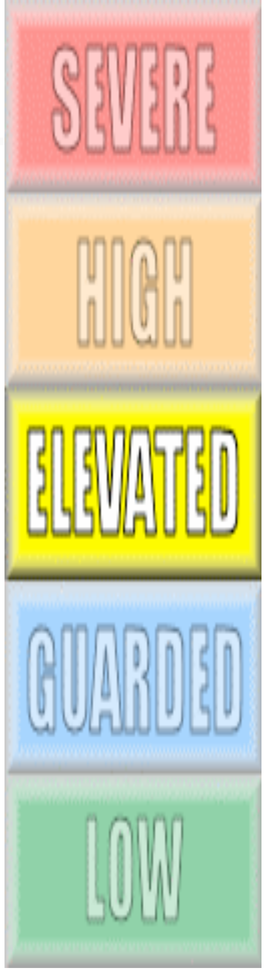
4. To: Different Layers:



LAYERS	DANGERS
HTTP Client / User	Cross-Site Scripting Spoofing/Trickery
Transport Layer HTTP(s)	Passive Monitoring Man-in-the-Middle Session Hi-Jack
Firewall	ALLOW HTTP(s)
Web Server	Buffer Overlow Format String Directory Traversal Default Accounts Sample Applications
Web Applications CGI's	Filter-Bypass Manipulation Metacharacters Null Characters Buffer Overflow
Firewall	Internal Network
Database	Direct SQL Commands Restricted Database Query Database Exploits

5. With: Common Attack Types & Threat Levels:





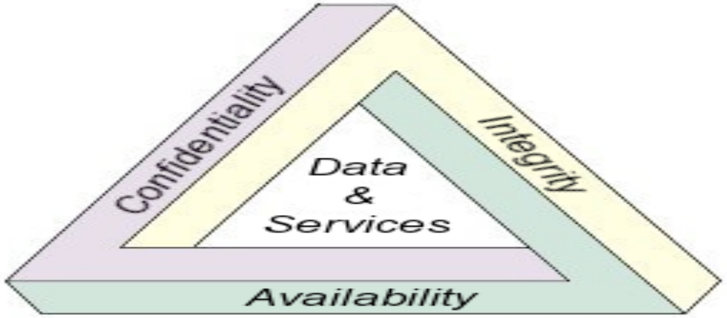
6. And: Your Best Operational Security Model is: Protection = Prevention + Detection + Response

Prevention

Access Controls

Firewall

Encryption



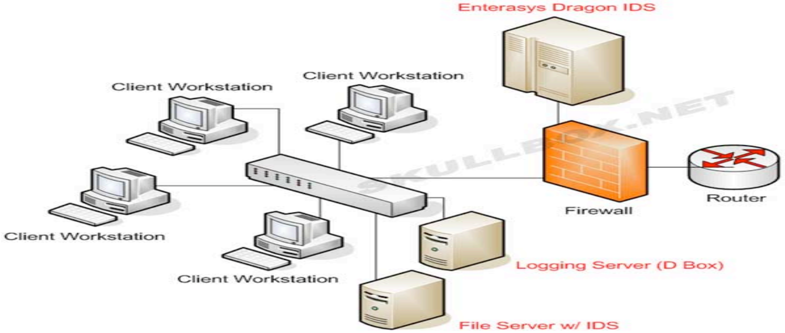
+

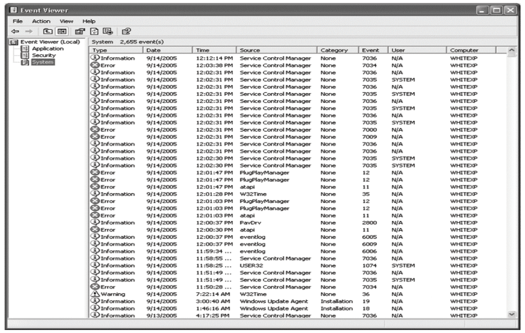
Detection

Audit Logs

IDS

Honeypots





System 2,655 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	9/14/2005	12:12:14 PM	Service Control Manager	None	7036	N/A	WHITEXP
Error	9/14/2005	12:03:38 PM	Service Control Manager	None	7034	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Error	9/14/2005	12:02:31 PM	Service Control Manager	None	7000	N/A	WHITEXP
Error	9/14/2005	12:02:31 PM	Service Control Manager	None	7009	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:30 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:30 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Error	9/14/2005	12:01:47 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:47 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:47 PM	atapi	None	11	N/A	WHITEXP
Information	9/14/2005	12:01:28 PM	W32Time	None	35	N/A	WHITEXP
Error	9/14/2005	12:01:03 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:03 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:03 PM	atapi	None	11	N/A	WHITEXP
Information	9/14/2005	12:00:37 PM	PavDrv	None	2800	N/A	WHITEXP
Error	9/14/2005	12:00:30 PM	atapi	None	11	N/A	WHITEXP
Information	9/14/2005	12:00:37 PM	eventlog	None	6005	N/A	WHITEXP
Information	9/14/2005	12:00:37 PM	eventlog	None	6009	N/A	WHITEXP
Information	9/14/2005	11:59:34 ...	eventlog	None	6006	N/A	WHITEXP
Information	9/14/2005	11:58:55 ...	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	11:58:25 ...	USER32	None	1074	SYSTEM	WHITEXP
Information	9/14/2005	11:51:49 ...	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	11:51:49 ...	Service Control Manager	None	7035	SYSTEM	WHITEXP
Error	9/14/2005	11:50:28 ...	Service Control Manager	None	7034	N/A	WHITEXP
Warning	9/14/2005	7:22:14 AM	W32Time	None	36	N/A	WHITEXP
Information	9/14/2005	3:00:40 AM	Windows Update Agent	Installation	19	N/A	WHITEXP
Information	9/14/2005	1:46:16 AM	Windows Update Agent	Installation	18	N/A	WHITEXP
Information	9/13/2005	4:17:25 PM	Service Control Manager	None	7036	N/A	WHITEXP

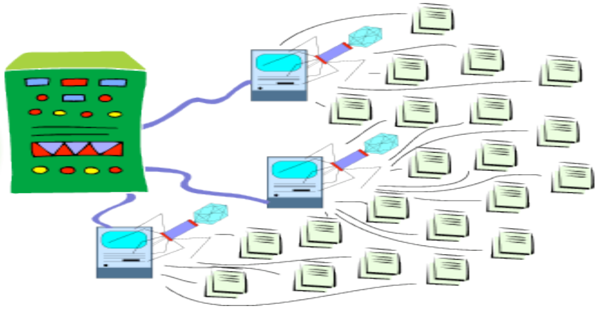
+

Response

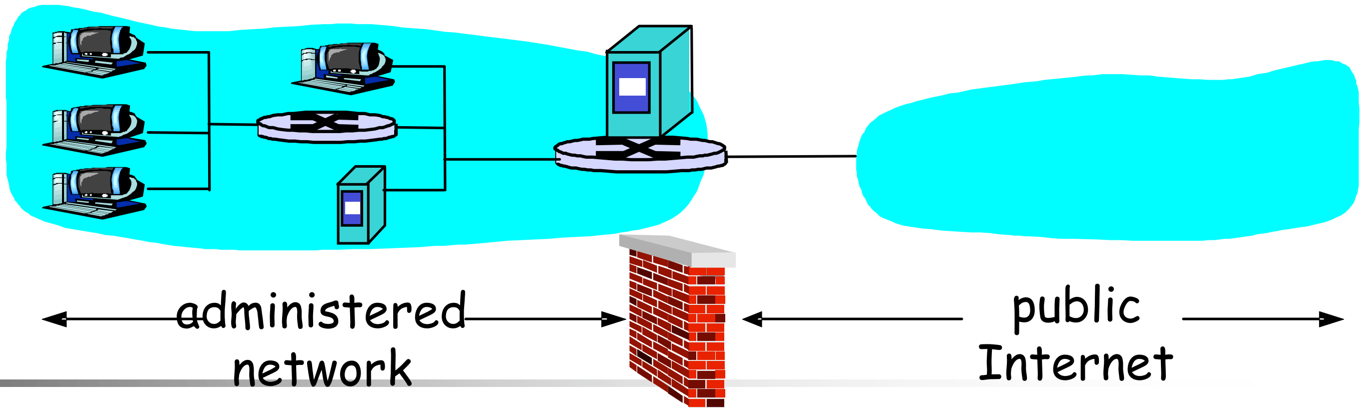
Backups

Incident Response

Computer Forensics



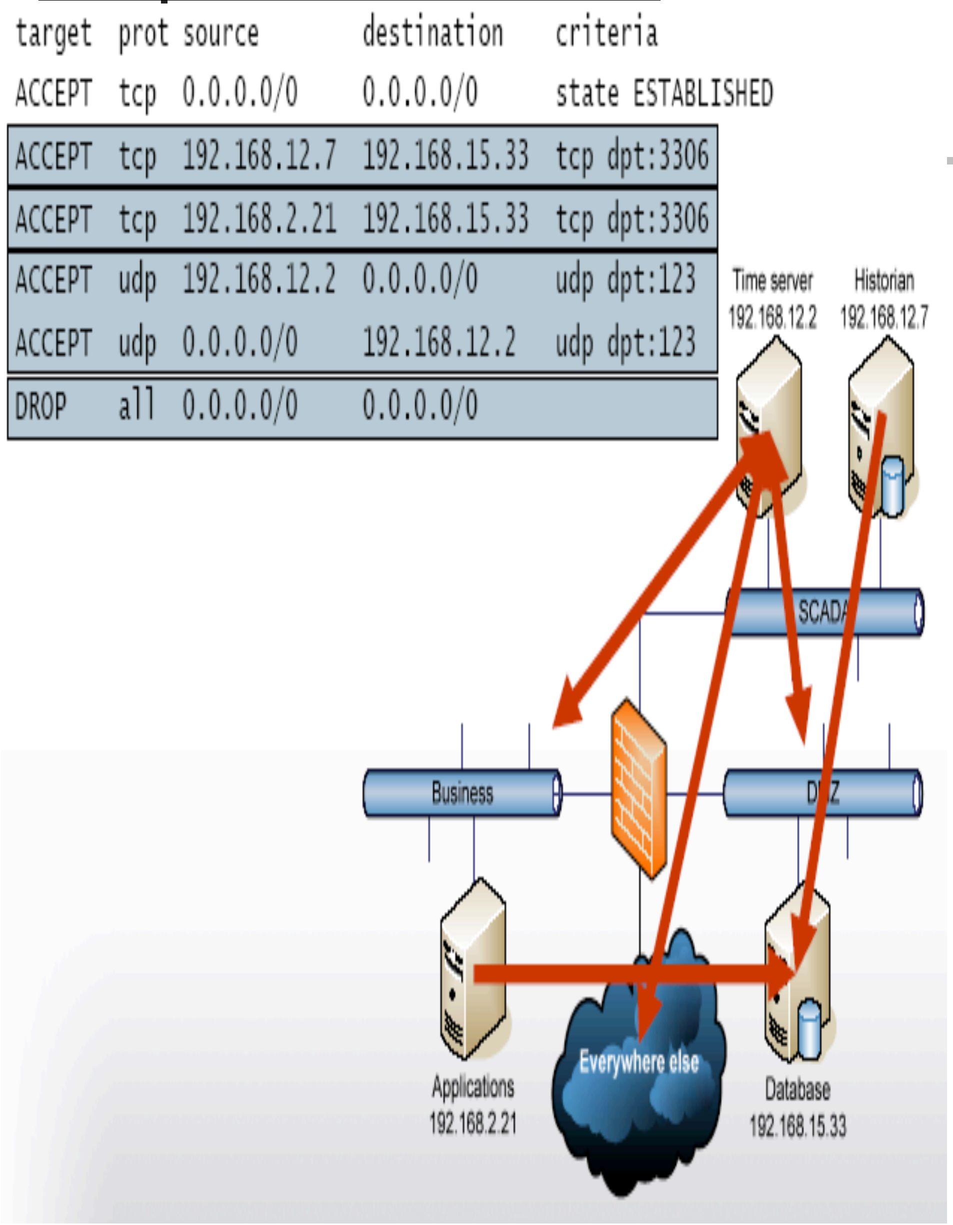
Firewall



- Job: Isolates organization’s internal net from Internet, allow some packets to pass and blocking others.
- Why:
- Prevent DoS Attacks: An attacker establishes many bogus TCP connections, no resources left for “real” connections. This is called SYN flooding.
- Prevent illegal modification / Access of internal data: An Attacker replaces CIA’s homepage with other
- Allow only authorized access to inside network: set of authenticated users / hosts
- Mitigate Port-Scanning & probing

- Rules:
- Traffic criteria:
  - Source and destination address, source and destination port, protocol, physical interface, rate …
  - Typically NOT application-level information
- Action to take:
  - Allow traffic to pass
  - Drop traffic without notification
  - Reject traffic with notification to source
- Policy:
  - Actions for traffic that does not match any criteria

FW Rule Ex.

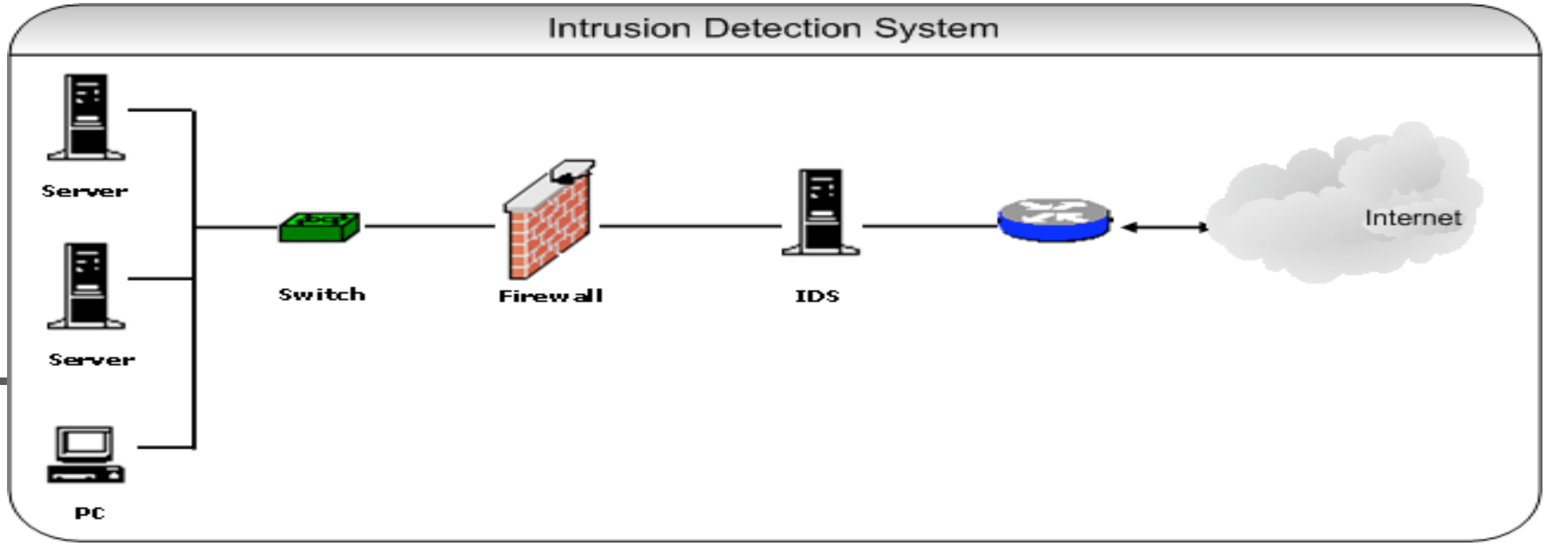


```
target  prot source        destination    criteria
ACCEPT  tcp  0.0.0.0/0     0.0.0.0/0      state ESTABLISHED
ACCEPT  tcp  192.168.12.7  192.168.15.33  tcp dpt:3306
ACCEPT  tcp  192.168.2.21  192.168.15.33  tcp dpt:3306
ACCEPT  udp  192.168.12.2  0.0.0.0/0      udp dpt:123
ACCEPT  udp  0.0.0.0/0     192.168.12.2   udp dpt:123
DROP    all  0.0.0.0/0     0.0.0.0/0
```

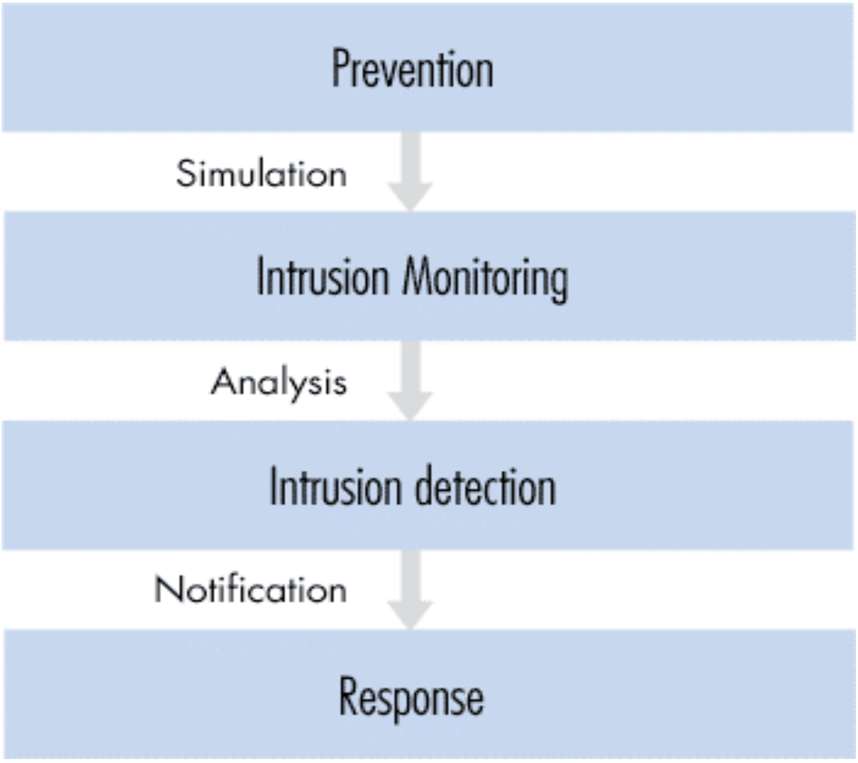
FW Pros & Cons

- PROS: A useful security tool that can:
  - Provide perimeter security
  - Implement security policy
- CONS:
  - Needs Careful design, configuration, and careful monitoring
  - It is ONLY a ONE link in the security chain
  - Provide little protection from insiders
  - Its failure can lead to network failure
  - May have vulnerabilities that intruders can exploit
  - IP spoofing: Router can NOT know if data really comes from claimed source

IDS



- IDS are expensive devices and called "Intelligent FW". They are more feasible within commerce. Combination of IDS and FW will provide maximum filtering of Network Traffic.
- Detects attacks on computer networks:
- Network-based Intrusion Detection NIDS:
  - Monitors real-time network traffic for malicious activity
  - Sends alarms for network traffic that meets certain attack patterns or signatures
- Host-based Intrusion-Detection HIDS
  - Monitors computer or server files for anomalies
  - Sends alarms for network traffic that meets a predetermined attack signature


Prevention

Simulation

Intrusion Monitoring

Analysis

Intrusion detection

Notification

Response

2nd :

Know The Mistakes!

Big Mistakes Spoken!

- We have antivirus software, so we are secure!
- We have a firewall, so we are secure!
- The most serious threats come from the outside!
- I do NOT care about security because I backup my data daily!
- Responsibility for security rests with IT security Staff! If I have a problem , they will fix it!
- CEO: We have budget constraints! Is security budget necessary that much as long as work is running?!

Security Breaches Mistakes:

IT Staff

- Connecting systems to Internet before hardening them & with Default accounts / passwords: The MOST common mistake!
- Using Telnet, FTP & unencrypted protocols for managing, routers, FW,
- Giving users passwords or changing it in response to telephone or personal requests when the requester is NOT authenticated.
- Failing to maintain and test backups.
- Implementing firewalls with rules that do NOT stop malicious or dangerous traffic-incoming or outgoing.
- Ignoring to implement or update virus detection software
- Ignoring to educate users on what to do when they see a security problem.

Seniors Executives

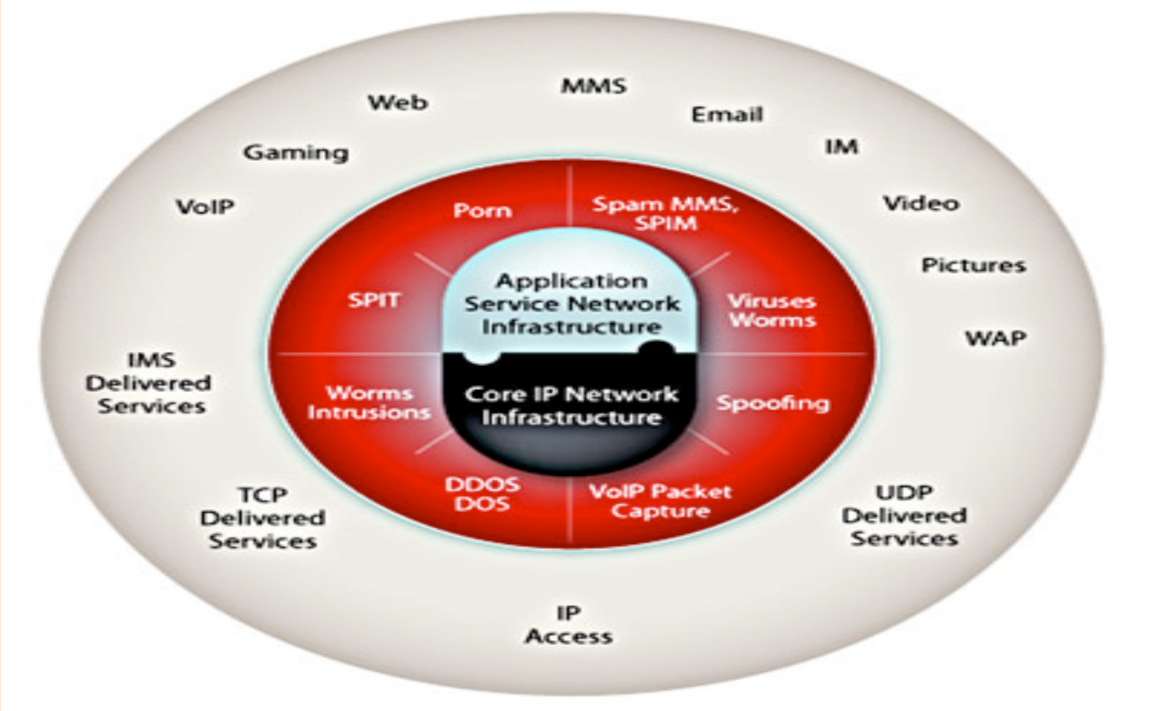
- Letting vendors define "good security"
- Underestimating the required security expertise
- Assigning untrained people to maintain security
- Failing to understand the relationship of information security & business and the bad consequences of poor information security
- Relying primarily on a firewall.
- Firstly think of budget concerns, neglecting the value of their information and organizational reputations.
- Authorizing reactive, short-term fixes so problems re-emerge rapidly.

3rd : Know The:

Enemy:

+

Threats:



The Enemy:

Can be:

- Determined Outsider:
  - Hacker or Corporate Espionage: Gain of valuable information or fame
  - Attacks from outside with no/little information
- Determined Insider:
  - Ex-employee: gain of valuable information or revenge
  - Attacks from inside with information about network internals
- Script Kiddy:
  - Unsophisticated attacker relying on scripts exploiting common vulnerabilities
  - Usually attacks random targets ("low hanging fruit")
- Automated Malicious Agent:
  - Fast-spreading worms such as Nimda demonstrated speed of automated agents
  - Quietly infect large number to strike others

Purposed For:

- Break in to systems:
  - To steal information
  - To manipulate information
  - To use resources
- Take control of systems:
  - To perform new attacks
  - To manipulate systems
- Disrupt service:
  - To extort target
  - To discredit target
  - To facilitate other attack

The Hackers:

Classes:

- Black Hats = Malicious intent
- White Hats = For defensive purposes / hacking countermeasures. Also called Ethical Hacker
- Gray Hats: Good Or bad!

5 Stage Attacks:

- Passive and Active discovery
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

The Threats: Always Increasing!

1. Virus, Worm, Spyware, Malware, etc
2. Port Scanning, Packet Sniffing, IP Spoofing
3. DoS= Denial of Service & DDoS
4. Wireless Security
5. Shared Computers, P2P
6. Zombie Computers, Botnet, Channels, etc
7. Insiders: The most unseen danger!
8. Lack of Policies, Regulations, Laws, Compliance, Auditing, etc

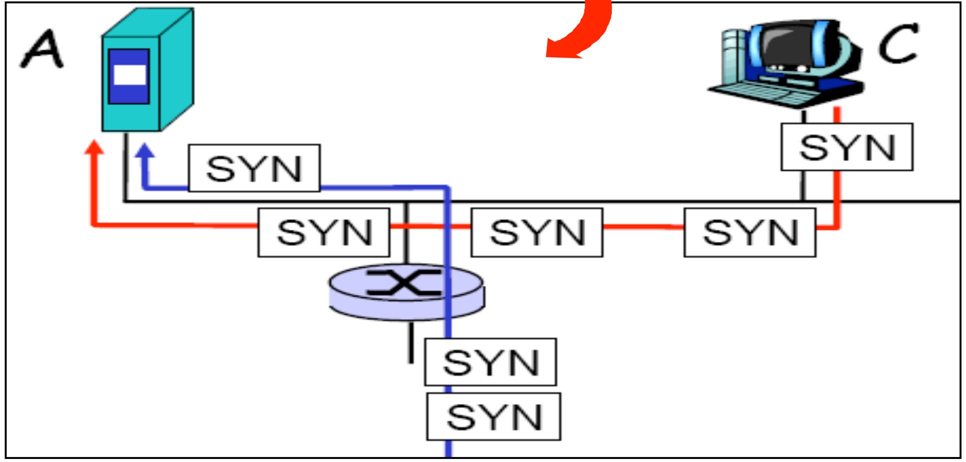
Threat Types: Examples

Port Scanning:

- Tries to establish TCP connection to each port looking for:
  - Open ports
  - Firewall Configuration
  - Known vulnerabilities
  - Operating system details
- Countermeasures:
  - Record traffic entering network
  - Look for suspicious activity (IP addresses, ports being scanned sequentially)
  - Port Scanners: e.g. nmap
  - Vulnerability Scanner: e.g. Nessus, Secunia, etc
  - Firewall ACL (Access Control List): e.g. firewalk

DoS:

- A flood of maliciously generated packets to swamp receiver. If multiple / coordinated packets, it is called Distributed DoS
- Countermeasures:
  - Filter out flooded packets (e.g., SYN) before reaching host
  - Traceback to source of floods
  - NetFlow

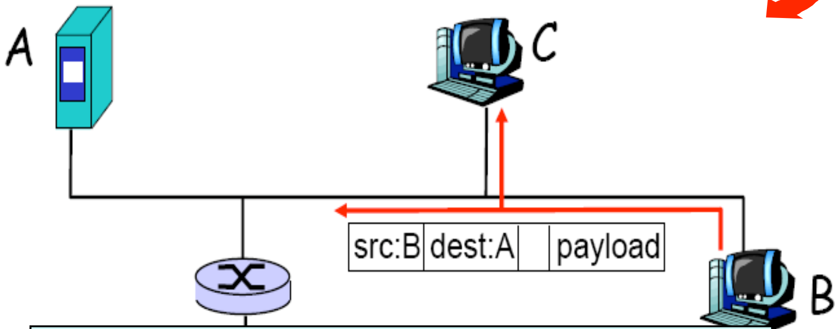


Example: C SYN-Attack A

Threat Types: Examples

Packet Sniffing:

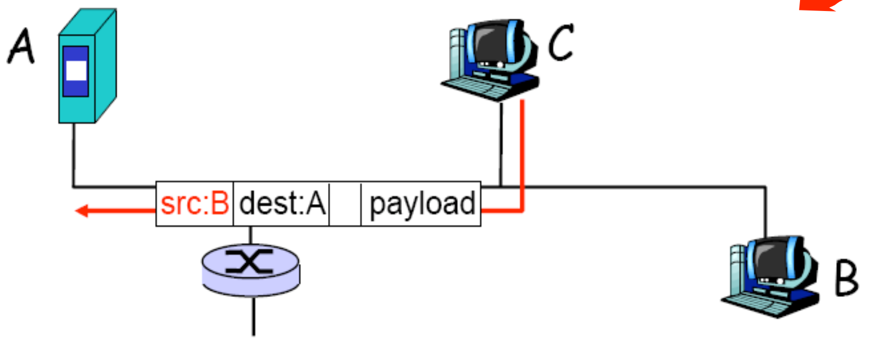
- A broadcast media, where Promiscuous NIC reads all packets and so the attacker can read all unencrypted data (e.g. passwords)
- Countermeasures:
  - All hosts in organization run software that checks periodically if host interface in promiscuous mode.
  - One host per segment of broadcast media (switched Ethernet at hub)



Example: C Sniff B Packets

IP Spoofing:

- Can generate “raw” IP packets directly from application, putting any value into IP source address field (to avoid being caught & bypass security tools), so the receiver can NOT tell if source is spoofed
- Countermeasures: Routers should NOT forward outgoing packets with invalid source addresses (e.g., datagram source address NOT in router’s network)



Example: C Pretend to be B

Threat Types: Security Threats Table

Security Area	Description	Why Important?	How bad is it?	Key Technologies
Spam	Unwanted Email / Traffic	Killer Application!	90% of email=Spam!	DNS, URI Block Lists
Malware	Malicious SW	Enterprise Sec. Undercuts	Faster than Vendors Patching!	AV, Secure Coding Practices, etc
Phishing	Reveal Accounts	E-commerce	Many Phished Sites	Browsers Alerts, Block Lists, Audits
DDoS	Traffic Floods	Most Worse for Security!	Entire Countries got offline!	Real time Hop-by-Hop Traceback
Encryption / Sniffing	Eavesdropping Sensitive Info.	Sniffed Passwords	Net. Monitoring	SSL, SSH, PGP, WAP2, VPN, Disk Enc.
Domain Names, IP, DNS, DNSSEC	Un-trusty Translation of Names to IP	All Network Application Trust DNS!	Entire Internet have to upgrade its Name-Servers	DNSSEC, Patch Name-Servers
Mobile Dev.	Enc. Challenges	More going Mob.	1.15 Billion sold(2007)	Dev./ Net. Encryption
Sec. Policies	Reg. / Comp.	PCIDSS for e.g.	Total Business Risk!	Depends on Enterprise!
DR / BC	Dis. Recovery	Bus. Continuity	Many do NOT have!	Offsite, Hot Site, Repl.
Awareness / Education	Be Ready!	Plan Ahead!	Many do NOT have!	Depends on Enterprise!

4th :

Start Your Security Roadmap & Learning

5 Technicalities:

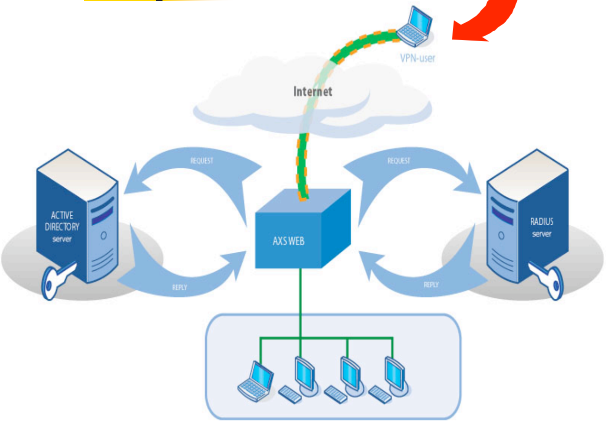
- Maintain Traditional Anti-Virus Protection
- Proactively Protect the Network
  - Behavioral Analysis
  - IPS / IDS
  - Check and Audit for suspicious activities
- Use Preventive Protection
  - Network Access Control
  - Safe, Effective Web Browsing
- Control Legitimate Applications and Behavior
  - Application Control
  - Application White listing
- Control and Encrypt Devices and Data
  - Encrypt All company Hard Drives

7 Milestones:

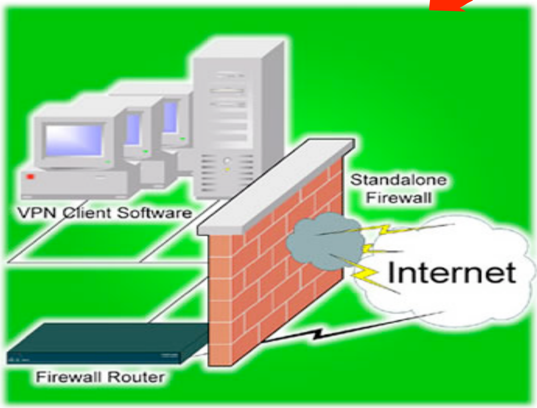
- Technology-Based Solutions
- Define Policies
- INFOSEC Team in every IT project
- Security System Life Cycle
- Compliance
- SETA: Security Education, Training Awareness for:
  - End Users
  - Technical Staff
  - Management, Executives & Board Members
- In-Depth Security (All Layers)

7 Milestones: 1. Technology-Based Basics:

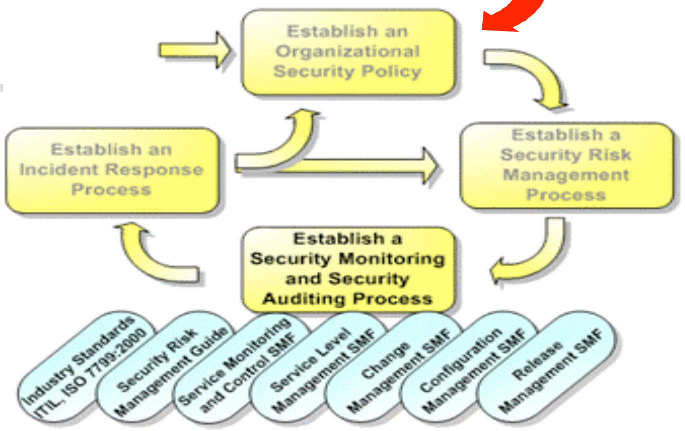
Authentication



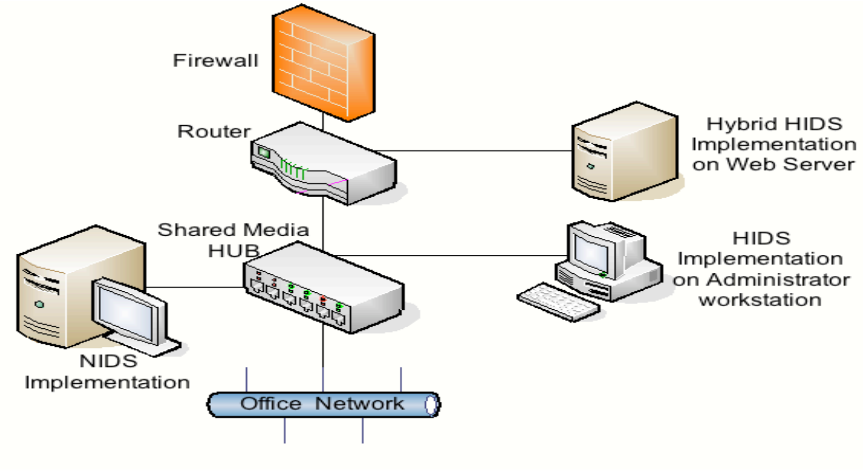
FW



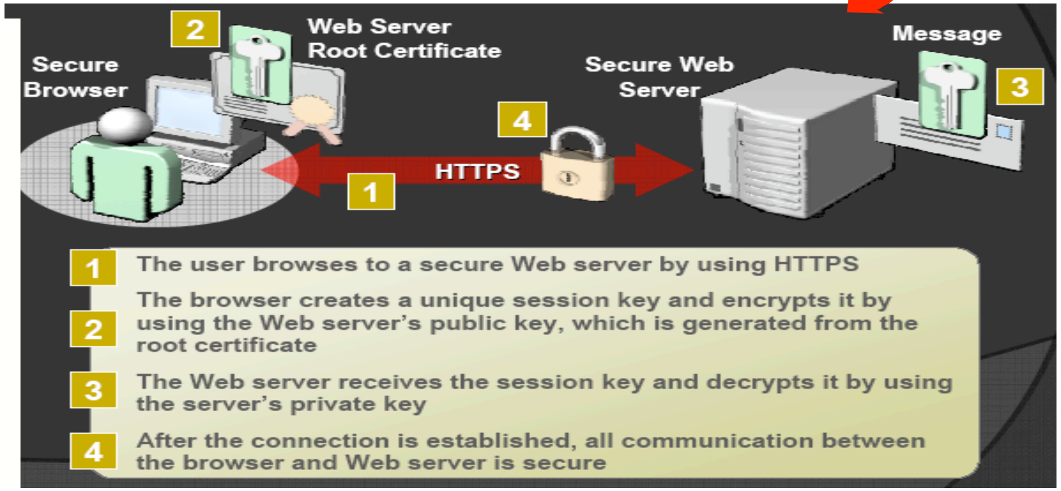
Auditing


Establish an Organizational Security Policy
Establish an Incident Response Process
Establish a Security Risk Management Process
Establish a Security Monitoring and Security Auditing Process
Industry Standards ITIL, ISO 7799:2000
Security Risk Management Guide
Service Monitoring and Control SMF
Service Level Management SMF
Change Management SMF
Configuration Management SMF
Release Management SMF

IDS / IPS


Firewall
Router
Hybrid HIDS Implementation on Web Server
Shared Media HUB
HIDS Implementation on Administrator workstation
NIDS Implementation
Office Network

SSL Secure Socket Layer



1 The user browses to a secure Web server by using HTTPS

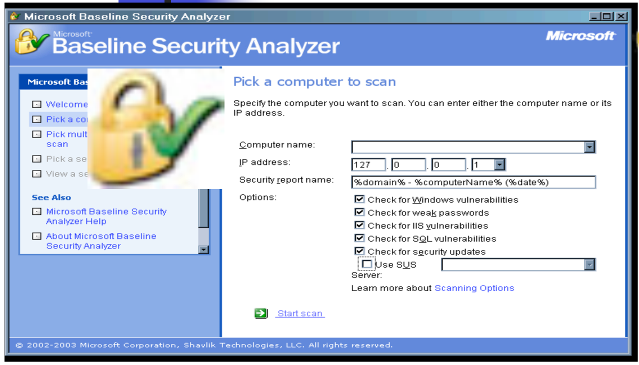
2 The browser creates a unique session key and encrypts it by using the Web server's public key, which is generated from the root certificate

3 The Web server receives the session key and decrypts it by using the server's private key

4 After the connection is established, all communication between the browser and Web server is secure

7 Milestones: 1. Technology-Based Basics:

Tools: Penetration Testing / Security Analyzers / Vulnerability Scanners/ Port Scanners / Packet Sniffers / Wireless / Web Scanners…etc


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Bas
Welcome
Pick a co
Pick mult scan
Pick a se
View a se
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Start scan
© 2002-2003 Microsoft Corporation, Shavlik Technologies, LLC. All rights reserved.

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Computer name:

IP address: 127 . 0 . 0 . 1

Security report name: %domain% - %computerName% (%date%)

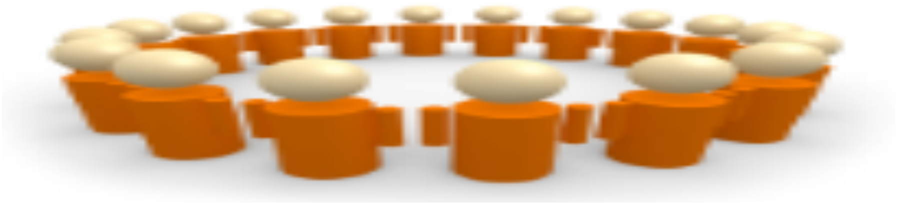
Options:
- ☑ Check for Windows vulnerabilities
- ☑ Check for weak passwords
- ☑ Check for IIS vulnerabilities
- ☑ Check for SQL vulnerabilities
- ☑ Check for security updates
- □ Use SUS Server:

Learn more about Scanning Options

7 Milestones:

2. Policies:

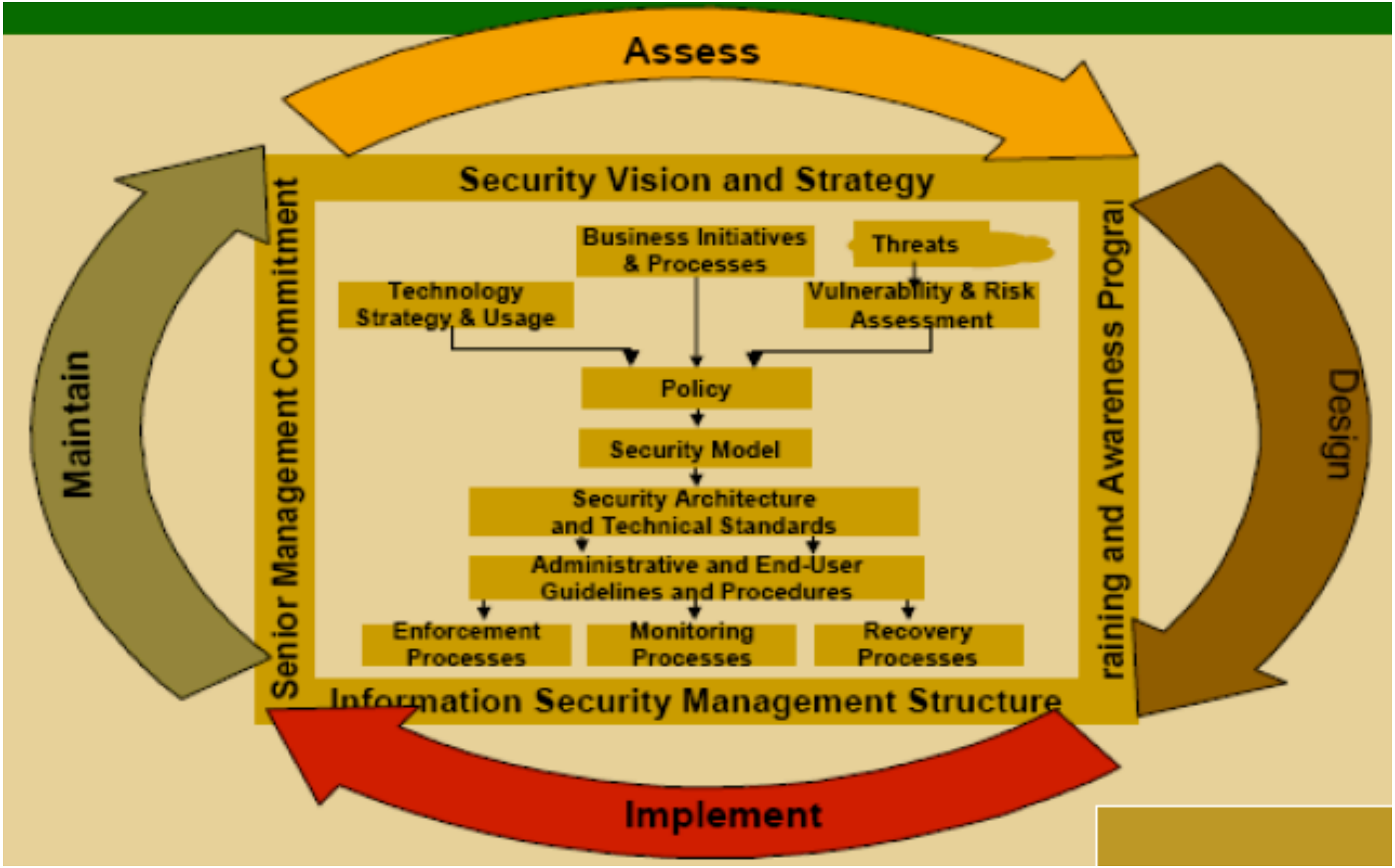
- Must be:
  - Designed with involvement of all stakeholders
  - Documented and Concise
  - Approved and supported by management
  - Understandable and Communicated
  - Enforced
- Most important ones:
  - AUP = Acceptable Use Policy
  - Change process and policy
  - Incident Response policy
  - Access Policy
  - Wireless Use Policy



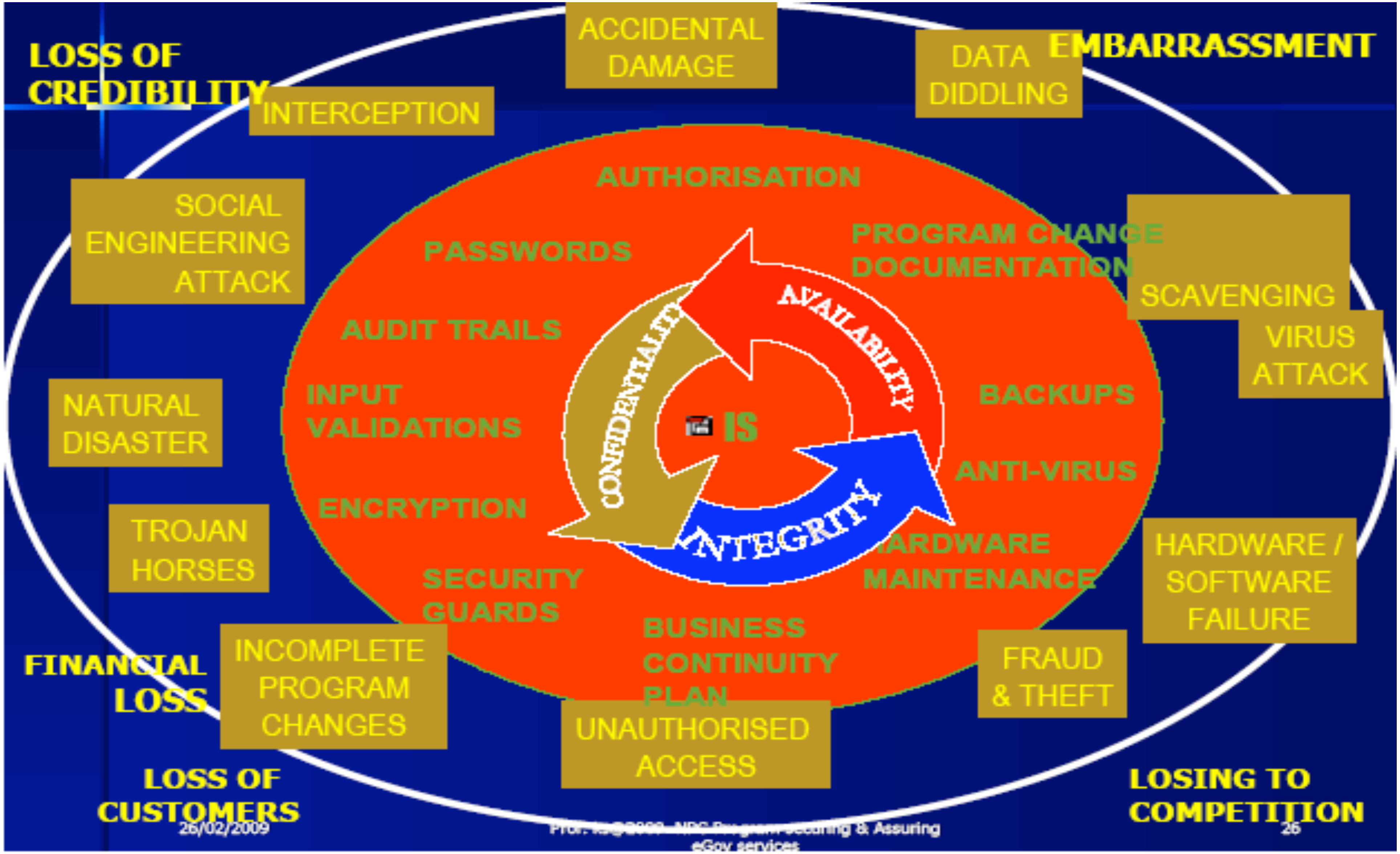
3. INFOSEC Team:

- INFOSEC team must be included at the start of each and every IT project.
- Security must be integrated into any system development.
- Make their role more public
- Conduct awareness campaigns
- Review their place in the organization chart.
- Have representation in upper management CISO (Chief Information Security Officer)

7 Milestones: Comprehensive Security Framework


Assess
Security Vision and Strategy
Business Initiatives & Processes
Threats
Technology Strategy & Usage
Vulnerability & Risk Assessment
Policy
Security Model
Security Architecture and Technical Standards
Administrative and End-User Guidelines and Procedures
Enforcement Processes
Monitoring Processes
Recovery Processes
Senior Management Commitment
raining and Awareness Progra
Information Security Management Structure
Maintain
Design
Implement

7 Milestones: Comprehensive Security Framework



LOSS OF CREDIBILITY

EMBARRASSMENT

FINANCIAL LOSS

LOSS OF CUSTOMERS

LOSING TO COMPETITION

ACCIDENTAL DAMAGE

DATA DIDDLING

INTERCEPTION

SOCIAL ENGINEERING ATTACK

SCAVENGING

VIRUS ATTACK

NATURAL DISASTER

TROJAN HORSES

HARDWARE / SOFTWARE FAILURE

INCOMPLETE PROGRAM CHANGES

FRAUD & THEFT

UNAUTHORISED ACCESS

AUTHORISATION

PASSWORDS

PROGRAM CHANGE DOCUMENTATION

AUDIT TRAILS

INPUT VALIDATIONS

BACKUPS

ANTI-VIRUS

ENCRYPTION

HARDWARE MAINTENANCE

SECURITY GUARDS

BUSINESS CONTINUITY PLAN

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

IS

26/02/2009

Prof. [illegible] NDC Program Securing & Assuring eGov services

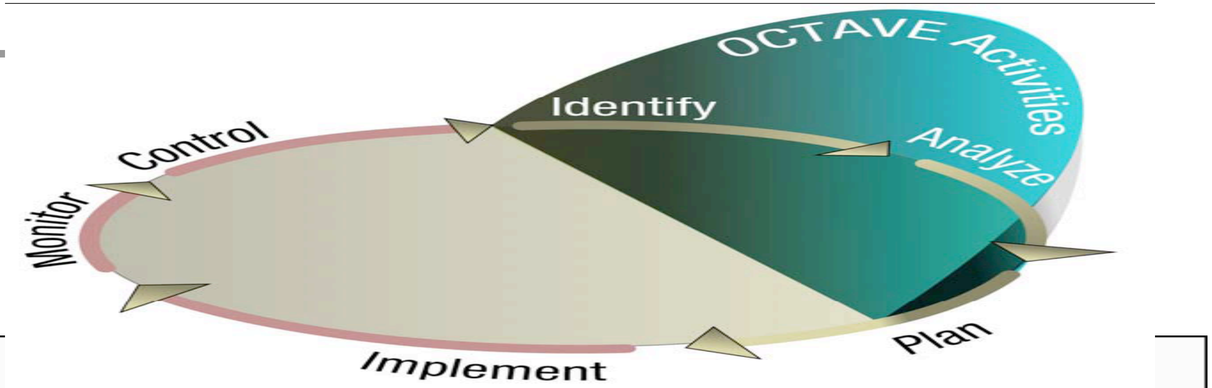
26

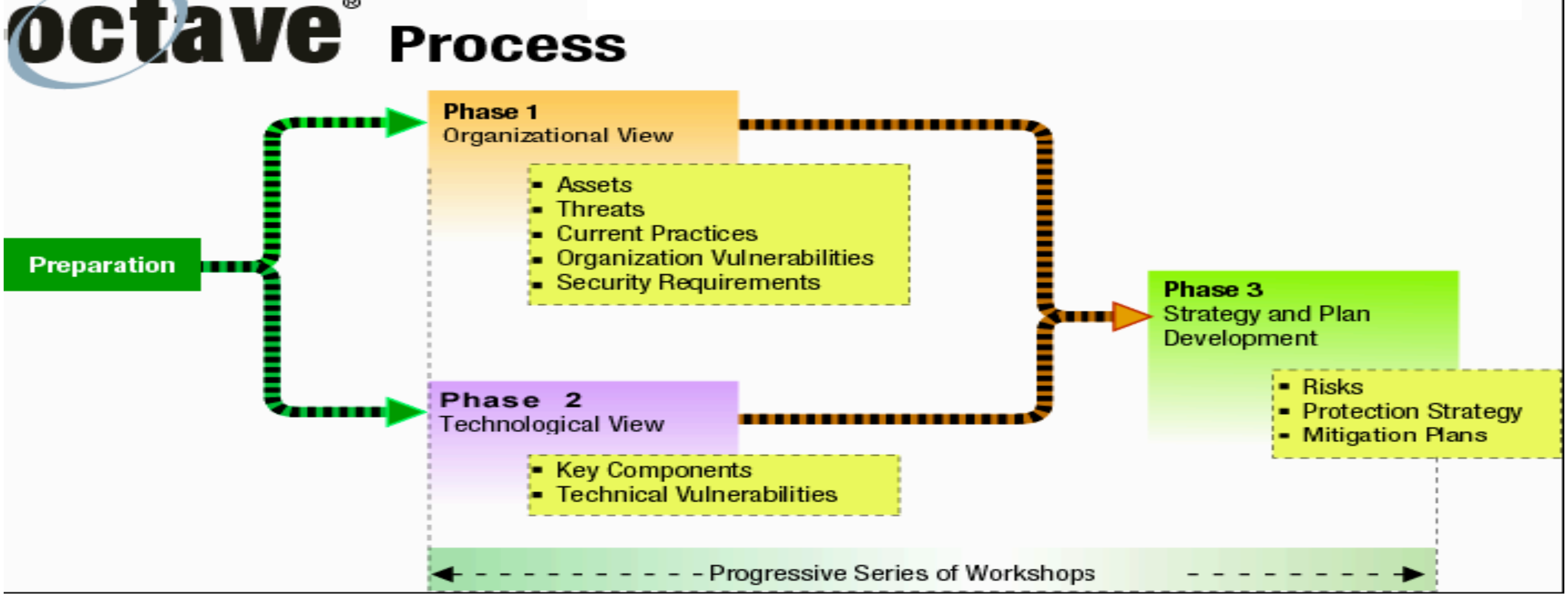
7 Milestones: 4. Security System Life Cycle

Example: CERT: Computer Emergency Response Team www.cert.org

OCTAVE:

Operationally Critical Threat, Asset, and Vulnerability Evaluation:





octave® Process

Preparation

Phase 1
Organizational View

- Assets
- Threats
- Current Practices
- Organization Vulnerabilities
- Security Requirements

Phase 2
Technological View

- Key Components
- Technical Vulnerabilities

Phase 3
Strategy and Plan Development

- Risks
- Protection Strategy
- Mitigation Plans

Progressive Series of Workshops

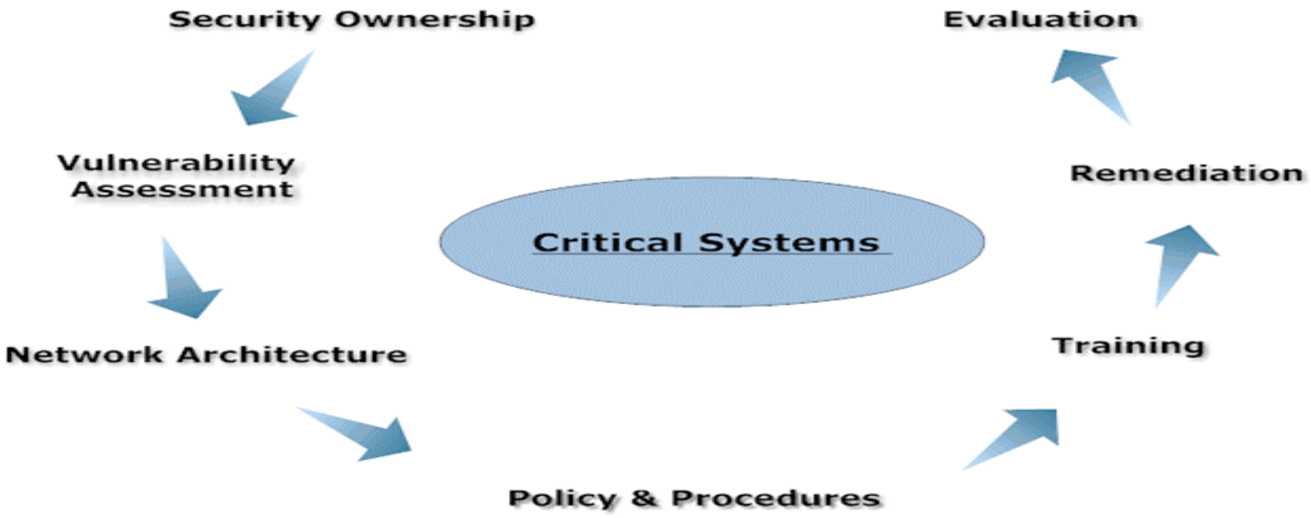
7 Milestones: 5. Compliance: Examples:

GLBA: Gramm-Leach-Bliley Act

- Require financial institutions to maintain response programs that specify reporting and other actions to take when access to customer information systems by unauthorized individuals is suspected or detected.
- 70 Federal Regulation 15736 (March 29, 2005)

Sarbanes-Oxley Act of 2002

- Requires public companies to use a broad framework of criteria against the effectiveness of their internal control systems. Internal controls must be in place to ensure integrity of the financial information. These controls must be established/regularly assessed.
- Some form of incident tracking and escalation is established for significant incidents.
- Provides protection for employees who report fraud.



7 Milestones: 6. SETA:

Security Education Training & Awareness

7. For End Users

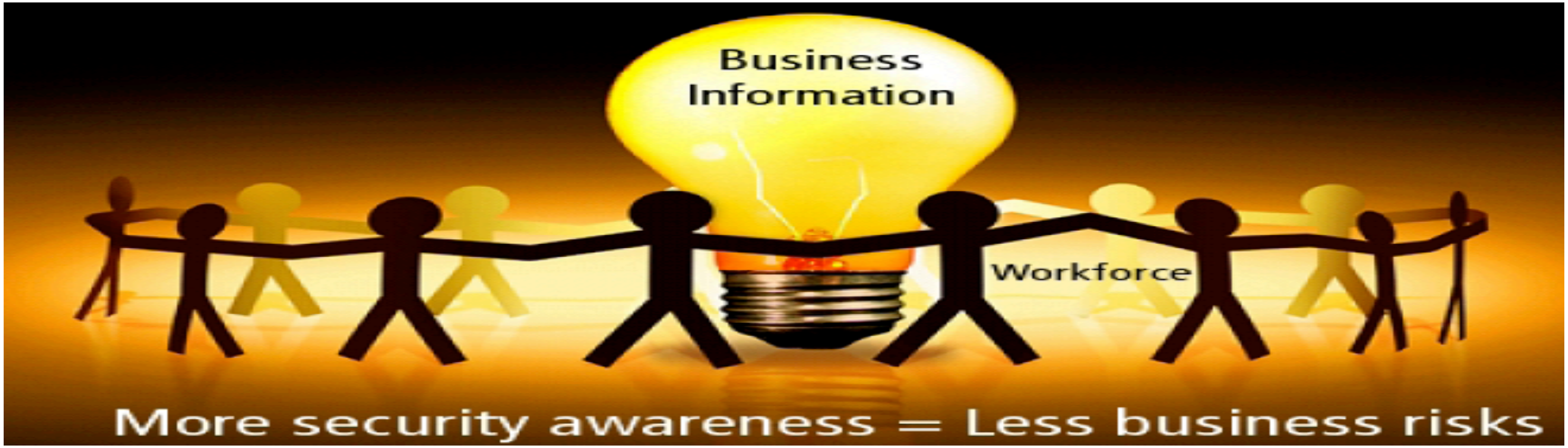
- Create a culture of security awareness (Posters, Slogans, etc)
- Make Security Policy: Readable / Understood and enforced

8. For Technical Staff

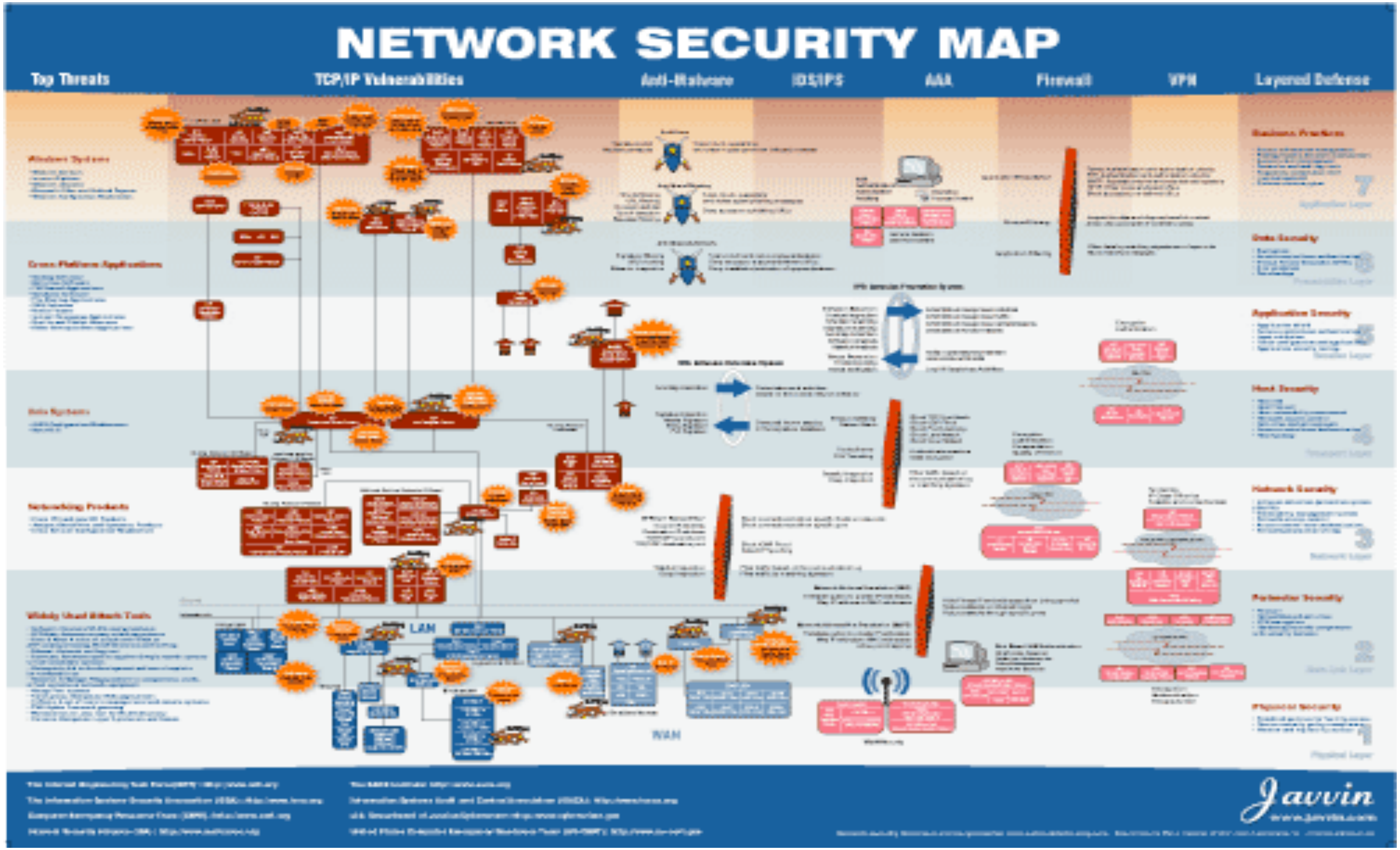
- Training: Compliance, Certifications, PPTs, Seminars, Memberships, etc
- Incidents Reporting's, Task Forces, etc

9. For Management:

- Incorporate security in business processes
- Compliance, Legal , Risk Assessments Trainings
- Make security part of Working Cultures



7 Milestones: 10. In-Depth Security



http://www.javvin.com/pics/SecurityMapM.gif

Keep abreast of Security Updates & "Who is doing What" via:

- Best Practices, Case Studies, White Papers,
- Mailing Lists, Discussion Forums, Groups, etc
- Seminars, Conferences, Tutorials,
- Webcasts, Webinars, Podcasts, etc
- Certifications, Learning paths, etc
- Ask The experts, Articles, etc
- International Bodies, entities, organizations,
- International Vendors, Solutions Providers, etc

A jungle of Security Expertise Out there!

- www.nist.gov
- www.cert.org
- www.sans.org
- www.ietf.org
- www.ripe.net
- www.isoc.org
- www.blachat.com
- www.hitb.org
- www.defoc.org
- www.educause.edu
- www.enisa.europa.eu
- www.hakin9.org
- www.internet2.edu
- www.isaca.org
- www.sectools.org
- www.owasp.org

- www.dshield.org
- www.hackerchoice.org
- www.techrepublic.com
- www.techtarget.com
- www.networkworld.com
- www.insecure.org
- www.sectools.org
- www.whitehatsec.ca
- www.darkreading.com
- www.circleid.com
- www.lightreading.com
- www.securityfocus.com
  www.about.com
- www.honeynet.org
- ARIN, AFNOG, APNIC…etc

……….And hundreds of others ! Stay Tuned!

Thanks For your Attention

Questions?