Gold Computing

HIPAA 201 - Securing Your Organization: A Technical Best Practices Overview

Robert Goldschmidt, PhD–CISSP–CISA
Information Security
Gold Computing, Portland OR
bob@goldcomputing.com 503-260-4046

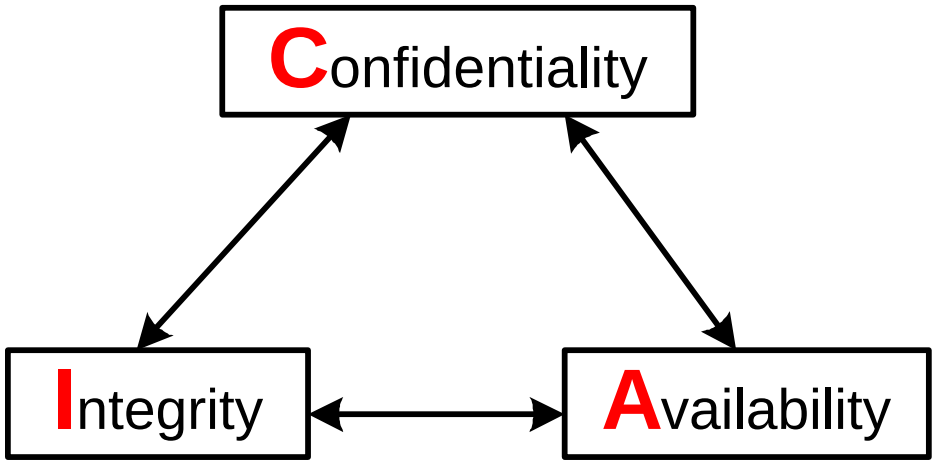
March 13, 2002

Agenda

- HIPAA Security Compliance Overview: Current Status
- Privacy versus Security: Peanut Butter and Chocolate
- HIPAA Security Compliance Requirements and InfoSec Generally Accepted Best Practices
- Security Policy Development
- Security Analysis
- Security and Technologies: Overview of Due Diligences
  - Communication and LAN Topologies
  - Protections
  - Detections
  - Responses

Information Security Basics: CIA

- Confidentiality
  - Assures that information is used only by those authorized to use it. Secret.
- Integrity
  - Assures that information is not changed without authorization. Safe.
- Availability
  - Assures that information is there when needed.



(ISC)² – CISSP Security Best Practices CBK

- Security Management
- Access Control
- Legal and Ethics
- Physical Security
- Business Continuity and Disaster Recovery Planning
- Security Architecture
- Cryptography
- Telecommunications and Network Security
- Applications and System Development
- Operational Security

ISC²: **http://www.isc2.org/cgi-bin/content.cgi?category=15**

CISSP Study: **http://www.cccure.org/index.php**

ISACA - CISA Info Audit Best Practices CBK

- Audit Process
- IT Management and Organization
- Technical Infrastructure and Operational Practices
- Information Security and

  1. Policies

     Access Control

     Network and Telecomm

     Encryption

     Physical

- Disaster recovery and Business
- Application Development and Acquisition,

  Management
- Business Process and Risk Management Analysis

isaca.org/cisacont.htm

HIPAA Security – High Matrix

- Contingency Plan
- Information access control
- Personnel Security
- Security Configuration Management
- Security Incident Response Procedures
- Security Management
- Termination Procedures
- Training
- Media Controls
- Physical access controls

Online Resources For InfoSec Best Practices

- **Best Practices in Network Security**
  http://www.networkcomputing.com/1105/1105f2.html
- **Commonly Accepted Security Practices & Recommendations**
  http://www.caspr.org/aboutcaspr.php
- **CERT® Security Improvement Modules**
  http://www.cert.org/security-improvement/#Harden
- **CISCO Network Security Policy: Best Practices White Paper**
  http://www.cisco.com/warp/public/126/secpol.html
- **Federal Best Security Practices**
  http://bsp.cio.gov/
- **Microsoft Security Best Practices**
  http://www.microsoft.com/technet/treeview/default.asp?url=
  /technet/security/bestprac/bestprac.asp
- **SANS Institute's Information Security Reading Room**
  http://rr.sans.org/index.php

Bob's InfoSec Best Practices Wheel

- Most important resource is people.
- Certification is based on implementation of both procedural and technical controls.
- Training. Training.
- Policies, process, planning, and documentation development is core to successful compliance.

Organization Security = CIA + Recovery

Gold Computing

Online Resources For Security Policy Development

- **NIST Internet Security Policy: A Technical Guide**
  http://csrc.nist.gov/isptg/html/
- **SANS Security Policy Project**
  http://www.sans.org/newlook/resources/policies/policies.htm
- **SANS Policies and Procedures**
  http://www.sans.org/newlook/resources/policies/bssi3/index.htm
- **Security Policies for the Internet**
  http://www.arnold.com/POLICIES_9512_SLIDES.HTML
- **Security Policy & Infrastructure**
  http://searchsecurity.techtarget.com/bestWebLinks/0,289521,sid14_tax281907,00.html
- **PentaSafe's Library of Information Security Publications**
  http://www.baselinesoft.com/

Security Analysis – No Free Lunches

- Business Impact
- Risk Assessment
- Vulnerabilities
- Architecture
- Required Services
- Penetration
- Intrusion and Log
- DR – BC

Technical Security Services – A Few Of My Favorite Things

- Routers
- Switches
- Firewalls
- Intrusion Detection
- Gateways
- Antivirus Management
- VPN
- Encryption
- Passwords
- Wireless
- Remote Access
- Box Configuration
- Patch and Update Management
- Access Control
- Authentication
- Configuration Management
- Backup and Restore
- Enterprise Integration-Correlation

Bob's Soapbox: About Technology

- Technology alone is NOT the solution.
- Judicious planning that leverages technology IS the solution.

ListServs and Email Notifications - 1

- **SecurityFocus Mailing Lists - BugTraq and others**
  http://www.securityfocus.com/cgi-bin/subscribe.pl
- **ComputerWorld**
  http://www.cwrld.com/nl/sub.asp
- **Information Security Magazine - Security Wire Digest**
  http://infosecuritymag.bellevue.com/
- **Network Computing and SANS - Security Alert Subscription**
  http://server2.sans.org/nwcnews/
- **Microsoft TechNet - Product Security Notification**
  http://www.microsoft.com/technet/treeview/default.asp?url=
  /technet/security/bull\etin/notify.asp

ListServs and Email Notifications - 2

- **NTBugTraq**
  http://www.ntbugtraq.com/
- **VulnWatch**
  http://www.vulnwatch.org/subscribe.html
- **Windows 2000 Magazine**
  http://www.win2000mag.net/Email/Index.cfm
- **Security Administrator - see the lower left side of the page**
  http://www.windowsitsecurity.com/
- **ZD-Net Security Updates**
  http://techupdate.zdnet.com/techupdate/filters/newsletters/sub/0,14214,6020424,0\0.html
- **Bruce Schneier's Crypto-Gram**
  http://www.counterpane.com/crypto-gram.html

About Patch and Update Management

- Huge volumes of notifications and patches.
- Configuration management, downtime, dependencies, FTE.
- Tools:
  - Microsoft
    - http://support.microsoft.com/default.aspx?scid=KB;EN-US;q303215&ID=KB;EN-US;q303215&
  - Commercial
    - http://www.bindview.com/products/Control/index.cfm
    - http://www.configuresoft.com/html_home.htm
    - https://www.ecora.com/ecora/solutions.asp#Security
    - http://www.shavlik.com/security/prod_hf.asp
    - http://www.patchlink.com/
    - http://grc.com/pw/patchwork.htm
    - http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

About SNMP Services and Community Strings

- SNMP services ubiquitous, hidden, enabled by default.
- Used for device status messaging and administration.
- Severe vulnerabilities have been found.
- Community strings – like passwords:
  - Public and Private
  - Read versus Read / Write
- Disable whenever and wherever possible.
- Service – Daemon location tools:
  - Foundstone / Freetools / Scanner / SNSscan
    http://www.foundstone.com/knowledge/free_tools.html
  - SANS SNMPing: http://www.sans.org/snmp.zip?70998269

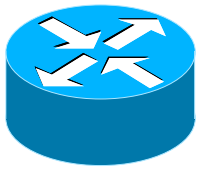
About Passwords

- Policies - Administrative / Procedures - Training
- Parameters:
  - Strength (length – complexity – creation methods)
  - Defaults and Blanks
  - Reuse
  - Lockouts
  - Storage
- Where – Everywhere:
  - All network and security devices
  - All servers and workstations
  - All database and client-server applications
  - All domain logins – native (AD, LDAP) and 3rd party (Radius, TACACS)
  - All email and messaging applications

About Anti-Virus Protection and Package Management

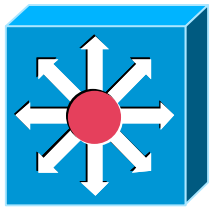
- Required on **ALL** workstations and servers. No excuses.
- Must be updated regularly and frequently. No excuses.
- Push versus Pull:
  - Clients pull DATs down from central sites. Email notification.
  - Push DATs to clients logon scripting.
- Centralized Management:
  - Server-based centralized administration.
  - Quarantine at the edge.
  - Push out new code and DATs.
  - Gateway support separate from server and desktop?
- But what about Remote Access?

Cisco Symbol Legend



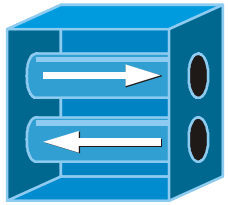
Router

Standard Switch

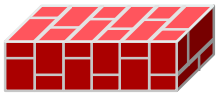


Large Switch

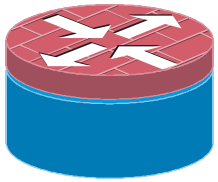
5500 family



VPN Concentrator

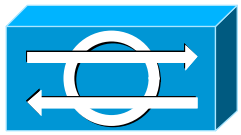


Firewall function



Router with firewall

Firewall

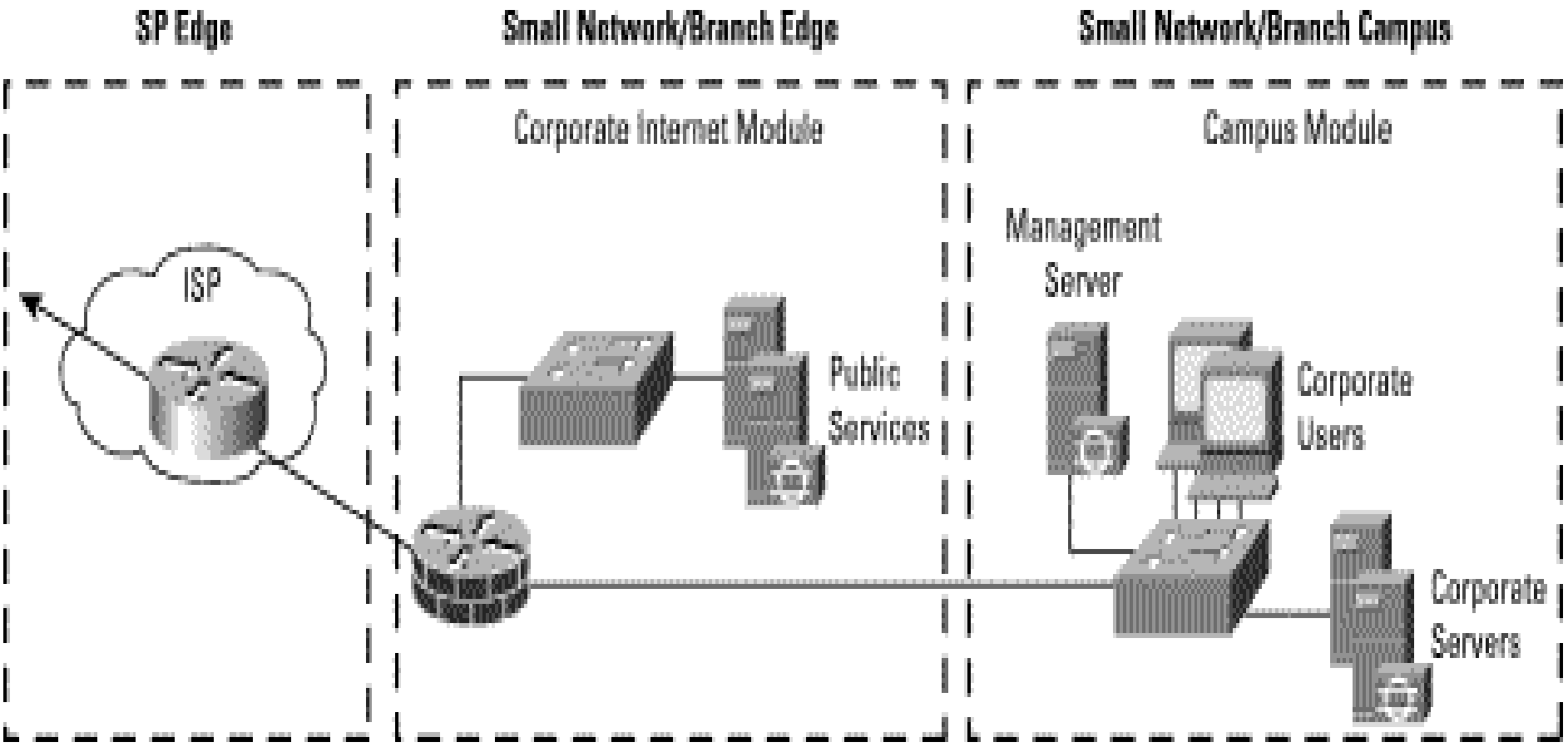


IDS / content filtration

Wireless access point

Gold Computing

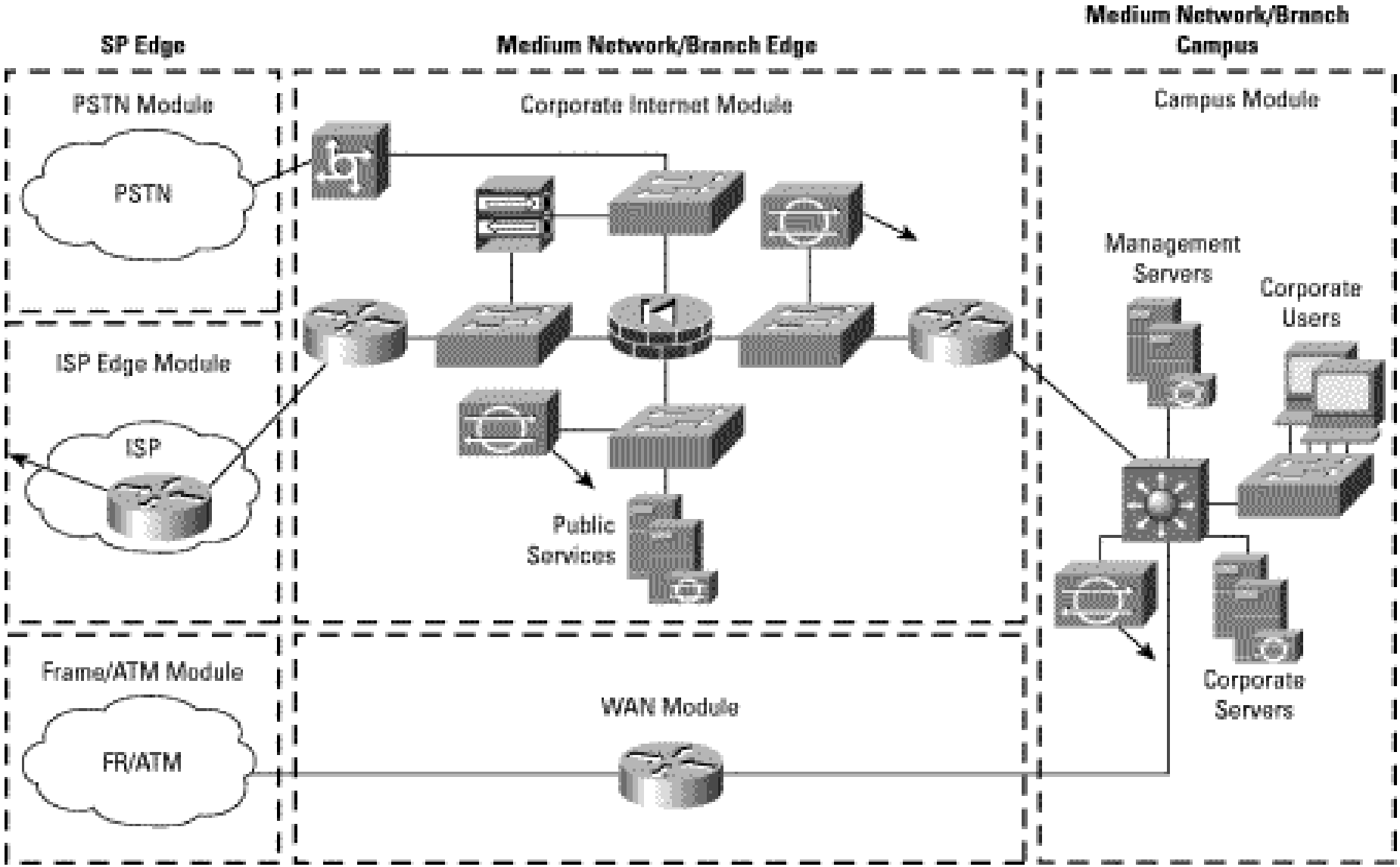
Network Overview – Small Infrastructure



CISCO Safe Blueprint:
http://www.cisco.com/warp/public/779/largeent/issues/security/safe.html

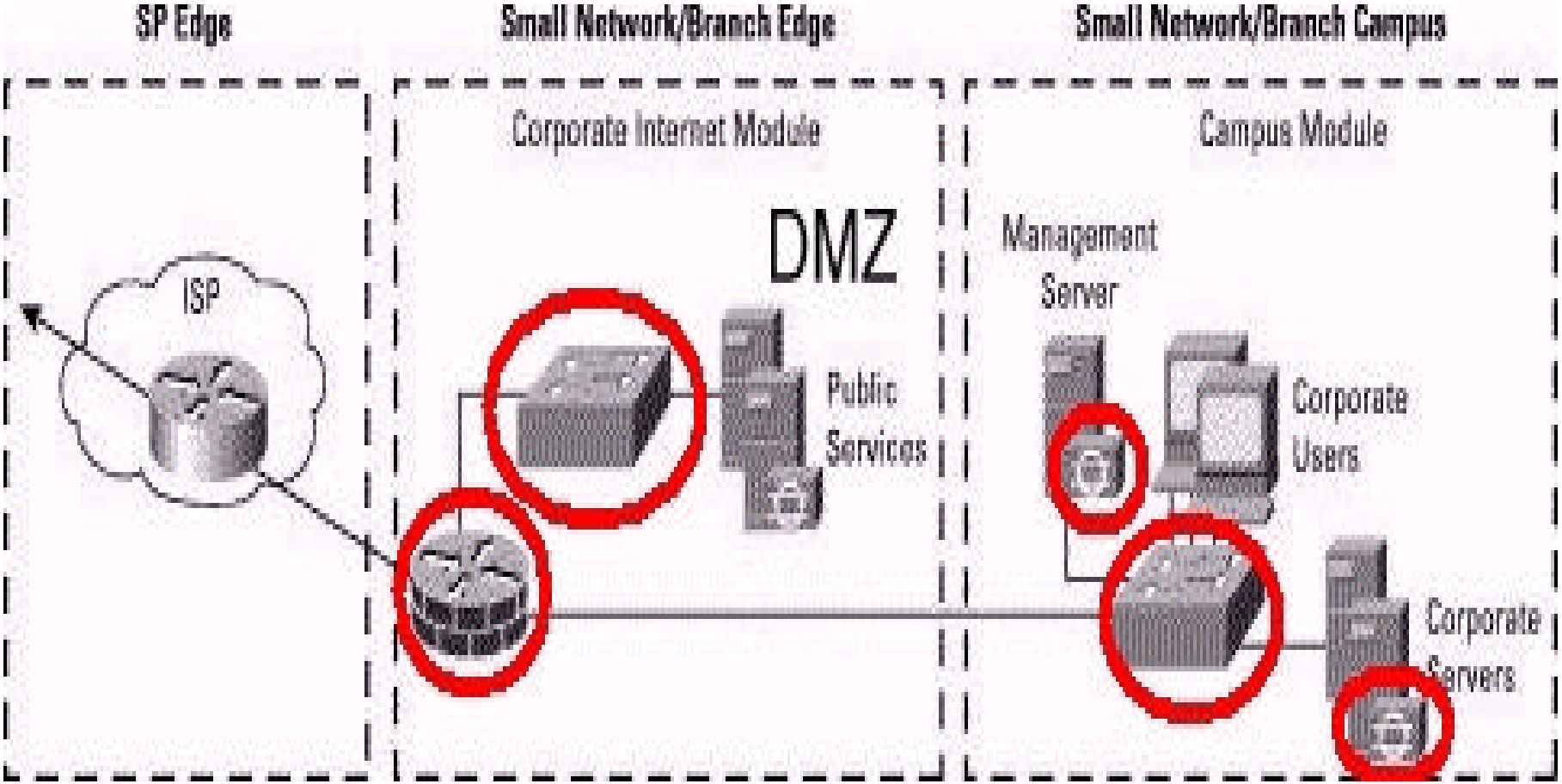
Gold Computing

Network Overview – Larger Infrastructure



Gold Computing

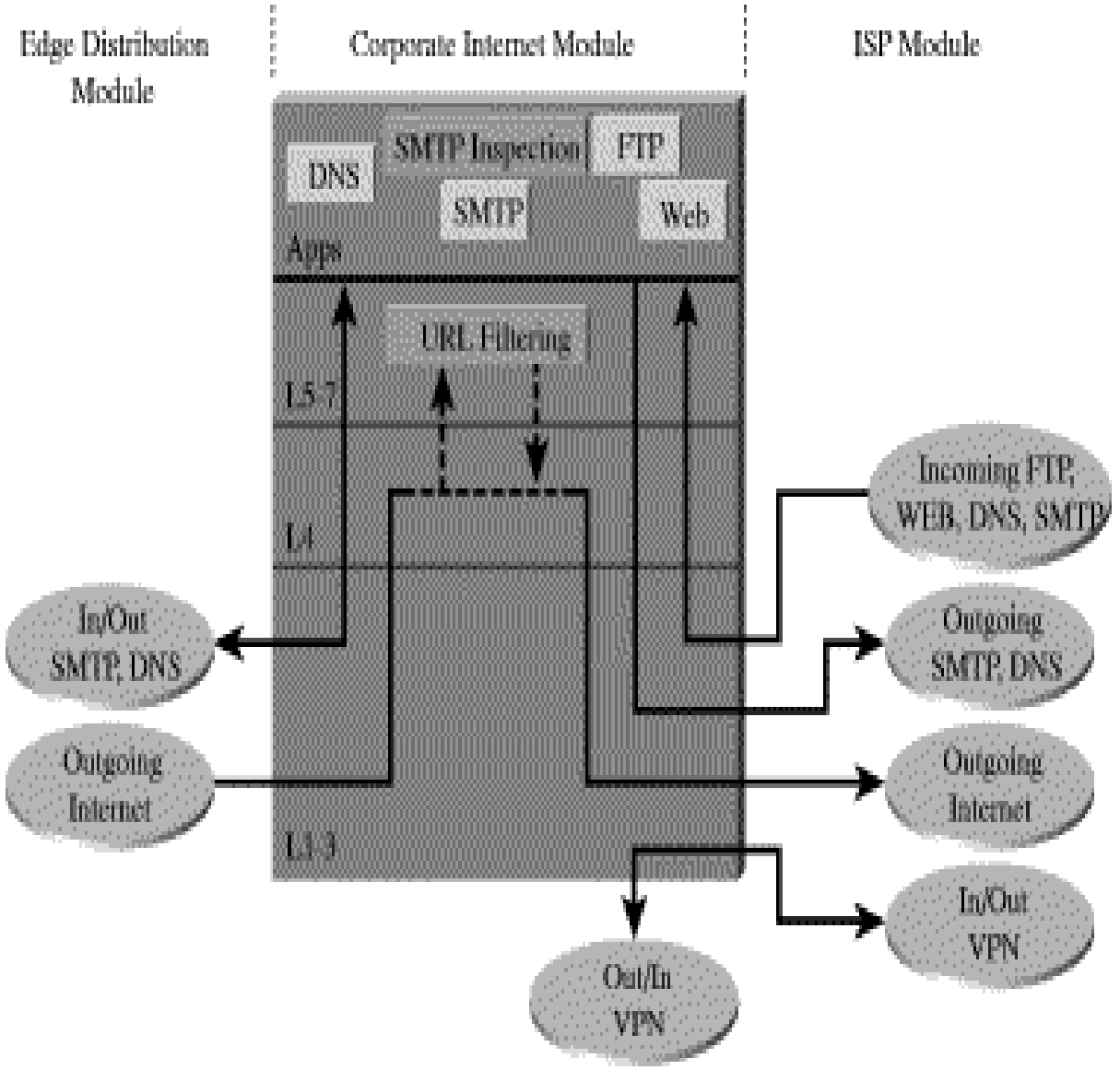
Network Control Points



Gold Computing

Your Network Traffic – What You Do Not Know Will Hurt You

- Many standard protocols
- More non-standard protocols
- All Internet-based applications require pass-through of required protocols
- Many vulnerabilities
- Default installations with unknown services



Gold Computing

About Routers

- Access Control Lists
- Anti-spoof capability
- Anti DoS capability
- Access level restrictions on management functions
- Configuration file management:
  - Saving copies
  - Managing versions
- Access methods:
  - Console
  - Telnet
  - SSH

About Switches

- Use of static ARP entries to servers and routers
- Disable Unused ports – set to non-routed LAN
- Enable and use VLANs for groups of servers
- Spanning ports for monitoring traffic?
- Managed?
  - If yes, access protocols
  - Authentication mechanism

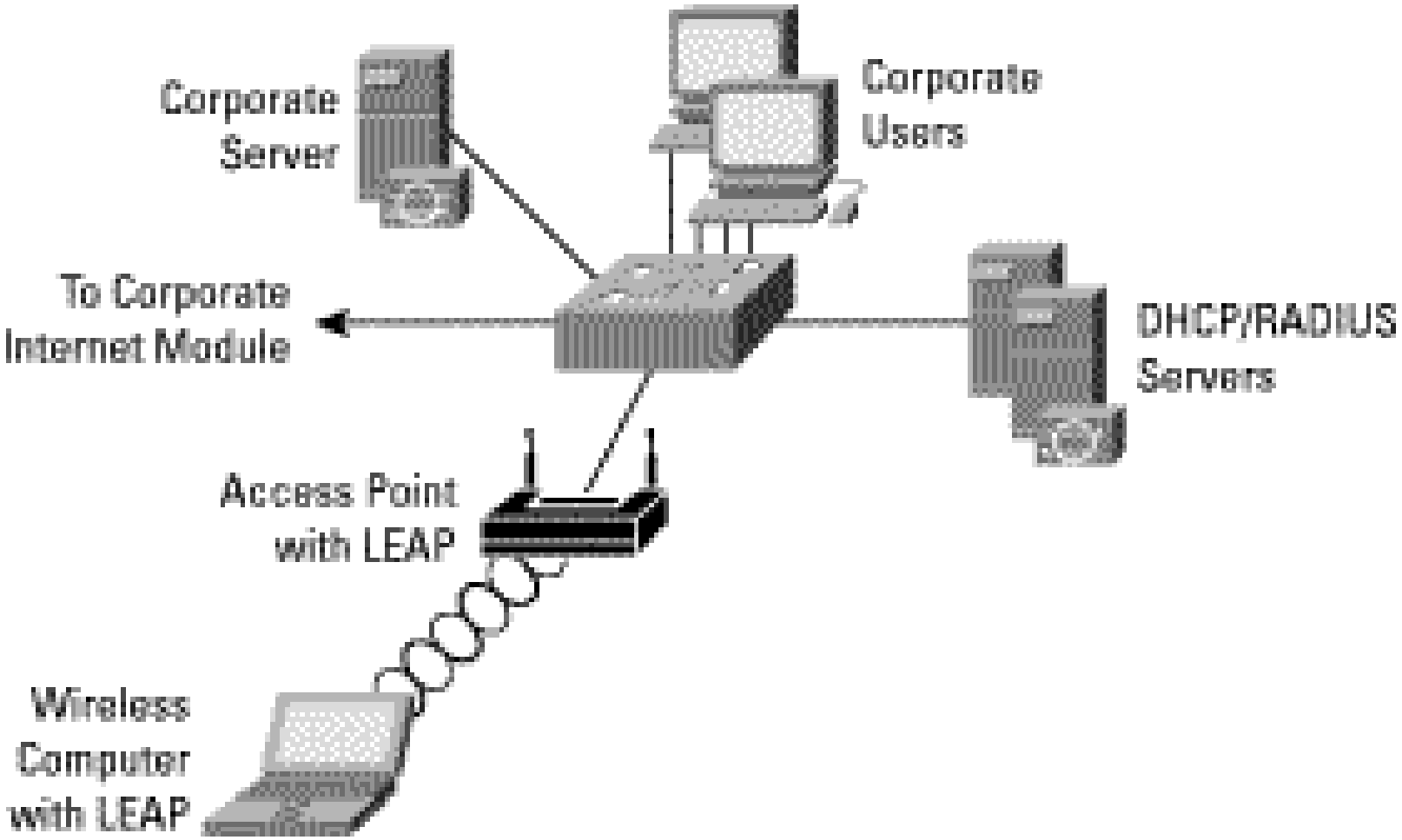
About Firewalls

- Many vendors: Checkpoint, Cisco, Netscreen, Watchguard
- Types: ASIC appliance, box appliance, standard OS
- To VPN or Not To VPN? That is the question.
- Rule Sets:
  - Know your services: Inside and Outside
  - Understand the required protocols: standard and non-standard
  - Anti-spoof
  - Filtration of source route packets
  - Prevention of inbound downloads by DMZ servers
  - Limiting initiation of outbound sessions by DMZ servers
  - Ingress versus Egress filtration

About Intrusion Detection

- Types:
  - Network
  - Host
- Costs of procurement:
  - Free, open source: NIDS = SNORT, HIDS = SNARE
  - Commercial: NFR, Cisco, Tripwire, Intrusion.com, ISS, **.....**
- Costs of administration:
  - FTE resources for administration
  - Log analysis
  - Event correlation and handling
- Tweaking and Tuning – To Avoid Tossing and Turning

Network Overview – Wireless Infrastructure



Gold Computing

About Wireless Access

- 802.11b has become increasingly popular.
- Serious vulnerabilities in WEP security implementation.
- Even more problems in standard implementation configurations.
- Recommendations:
  - WEP must be enabled. Use 802.1X implementation if possible.
  - Use authentication mechanisms: Radius, LDAP, TACACS, Cisco LEAP
  - Make all wireless traffic encrypted via mandatory use of VPN tunnels.
  - Use strong (non-default) SSID strings. Change as often as practical.
  - Disable wireless administration of access point – internal wired only
  - IP Allocation:
    - Disable DHCP allocation. Require static IPs that are centrally allocated.
    - Use MAC address verification (if available on access point).
    - Use non-default IP subnet classes.

About Remote Access - 1

- Remote access bypasses standard security controls.
- Diseases caught outside the enterprise brought inside.
- Recommendations:
  - Very strong Remote Access policies.
  - Very strong login authentication routines and technologies.
  - Use of desktop firewalls and most current anti-virus mandatory:
    - System certified as clean prior to installing software and allowing VPN access.
    - Firewalls must be bi-directional.
    - Anti-virus and firewalls must be running at all times.
    - Must be updated weekly.
  - Centrally managed desktop firewalls: Checkpoint, Sygate, Zonelabs
  - Trojan Scanning Tools:
    - http://www.moosoft.com/
    - http://onlinescanner.com/

About Remote Access - 2

- Many remote access IP-based protocols:
  - HTTP, SHTTP / SSL, Telnet, SSH, FTP, TFTP, MS Terminal Services
- Many not encrypted – use SSH and SSL where possible.
- Disable and disallow remote access where possible.
- Disallow – in Policy and Practice – all anonymous access.
- Separate Read from Read-Write storage areas.
- Modems pools – enable call-back features.
- Disallow – and check for – rogue modems. War dialing.
- Allow remote control software only under special circumstances.

About Logs

- Logging Devices: Routers, Firewalls, IDSs, Servers, VPNs.
- Huge amounts of data.
- Distributed repositories.
- Centralization – Integration – Event Correlation.
- Syslog services:
  - Log data in central storage area
  - OOB analysis
  - Encrypted in transit if possible
  - Encrypted locally if possible
  - Limit access to syslog server and logs
  - Append only
  - Network time synchronization: Simple Network Time Protocol (SNTP)

About Log Analysis and Enterprise Device Management

- Log Analysis Tools:
  - http://www.secadministrator.com/articles/index.cfm?articleid=15988
  - http://www.opensystems.com/
  - http://www.webtrends.com/products/firewall/frc.htm
- Enterprise Management and Analysis Packages:
  - http://www.esecurityinc.com/main.asp
  - http://www.iss.net/products_services/
  - http://www.intrusion.com/products/productcategory.asp?lngCatId=17
  - http://www.open.com/htm/products.htm

About Vulnerability Assessment Tools - 1

- Automated tools for assessing configuration and holes.
- Exploit database driven – must be maintained.
- Use with caution – and always provide warning.
- Tools – General Purpose:
  - Free, open source: Nessus, SARA, SAINT
  - Commercial:
    - CyberCop, Retina, STAT, ISS, NetRecon, NetIQ
    - Licensing issues
  - Reviews of these products:
    - http://www.networkcomputing.com/1201/1201f1b1.html
    - http://www.nwfusion.com/reviews/2002/0204bgrev.html

About Vulnerability Assessment Tools - 2

- **Other General Vulnerability Assessment Tools:**
  - http://www.cerberus-infosec.co.uk/cis.shtml
  - http://www.gfi.com/languard/lanscan.htm
  - http://www.qualys.com/services/index.html
- **IIS Checkers:**
  - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp
  - http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32571
  - http://www.kavado.com/ProductsScando.htm
- **Online testers - numerous tools, many are limited in ability.**
- **Port Scanners - scan external ports looking for listening services:**
  - http://www.insecure.org/nmap/
  - http://nscan.hypermart.net/
  - http://www.eeye.com/html/Research/Tools/nmapNT.html
  - http://www.sdesign.com/securitytest/index.html
  - Foundstone / Freetools / Scanner / SUPERscan
    http://www.foundstone.com/knowledge/free_tools.html

About Authentication and Access Control

- Native Single Factor – ID and Password:
  - Active Directory
  - LDAP
  - Kerberos
- Third-Party Single factor:
  - Radius
  - TACACS+
  - Diameter
- Strong 2-Factor, Something You Know, You Have, You Are:
  - Tokens and Smart Card Systems
  - Biometrics: iris, fingerprint, keyboard entry, retinal, voice print
  - Hardware biometrics
- PKI and Digital Certificates – A story for another day.

Incident Reponses

- DoS and DDoS – Difficult To Deal With:
  - Enable filtering on routers and firewalls. Cisco Shunning.
  - The farther upstream you protect, the better off you are. Your upstream pipe can still fill up. Get your ISP to filter for you.
  - Downstream liability is becoming a significant legal issue.
  - Reverse firewalls can help prevent outbound DoS streams.
- Standard Response Due Diligence:
  - Response Teams.
  - Scenario-based planning and testing.
  - Availability of alternative production and testing resources.
  - Availability of backup data.
  - Time windows for critical service recovery.
  - Disaster Recovery – Business Continuity Planning.

Backup and Restore

- Huge area of expertise and technology.
- A story for another day.
- Some issues:
  - Frequency and types of backups
  - Local versus Remote
  - Tape versus Electronic Vaulting
  - Tape administration: rotation, testing, local storage, off-site storage
  - Staff resources available: bodies and training
  - Restore reliability
  - Restore data availability during incident / disaster

A Few More Of My Favorite Things - More Security Stories For Another Day

- Configuration Issues: Desktop, Server
- VPN Access
- Encryption: tools, usage, PKI, e-signatures and the law
- Access control – additional topics: RBAC, physical
- Gateways: proxies, content filtration, email protections
- Employee usage monitoring
- Privacy: non-HIPAA
- Security awareness training
- Disaster Recovery – Business Continuity

Getting It Right

- Very Complex.
- Moving Target.
- Requires resources and support.
- Details Details ……
- Process oriented.
- Not rocket science, *BUT*

Thank You For The Privilege Of Addressing You

Robert Goldschmidt, PhD–CISSP–CISA
Information Security
Gold Computing, Portland OR
bob@goldcomputing.com (C) 503-260-4046