Security for Large-Scale LAN Design

Internet Security Systems K.K.

CIO, Executive Security Analyst

Masakazu Takahashi

- Session Description:

  An introduction of network design and technology to prevent damage from worms and other security incidents based on an actual case study.

Changes in Network Environment

Examples

	Around 2000 (Incident Response)	Since 2003 (Incident Operation)
Security Incidents are…	**May NOT happen** （reactive response）	**May Happen** （preemptive action） ・Many Cases are reported ・Network dependency
Position of Open Systems （Required Quality）	**“SHOULD” Systems and Networks** ・Auxiliary use ・Hobbies	**“MUST” Systems and Networks** ・EC-site, Online Banking, Governmental ・Mail, Web, Phone(VOIP) ・Product lines in Factories, mission-critical system
System Environments	**Develop, Dedicate** ・Dedicated and Proprietary Systems and Networks. ・Users had control	**Products, Combinations, Internet** ・Combination of Commercial Hardware, OS, Middleware, Applications. ・Users don’t have control
Control and Action	**User could control their systems/Networks** ・Especially, power user knew about their systems and networks well and were in control	**User can not control them, need many supports** ・Need to work with Hard ware, OS, Middle ware(ex. DB), application vendors.
Attackers	**Basically, Crime for pleasure** ・Defacing Home Pages, Viruses, Worms.	**Professionals** ・Phishing, Bot-net, adware, spyware ・intimidation

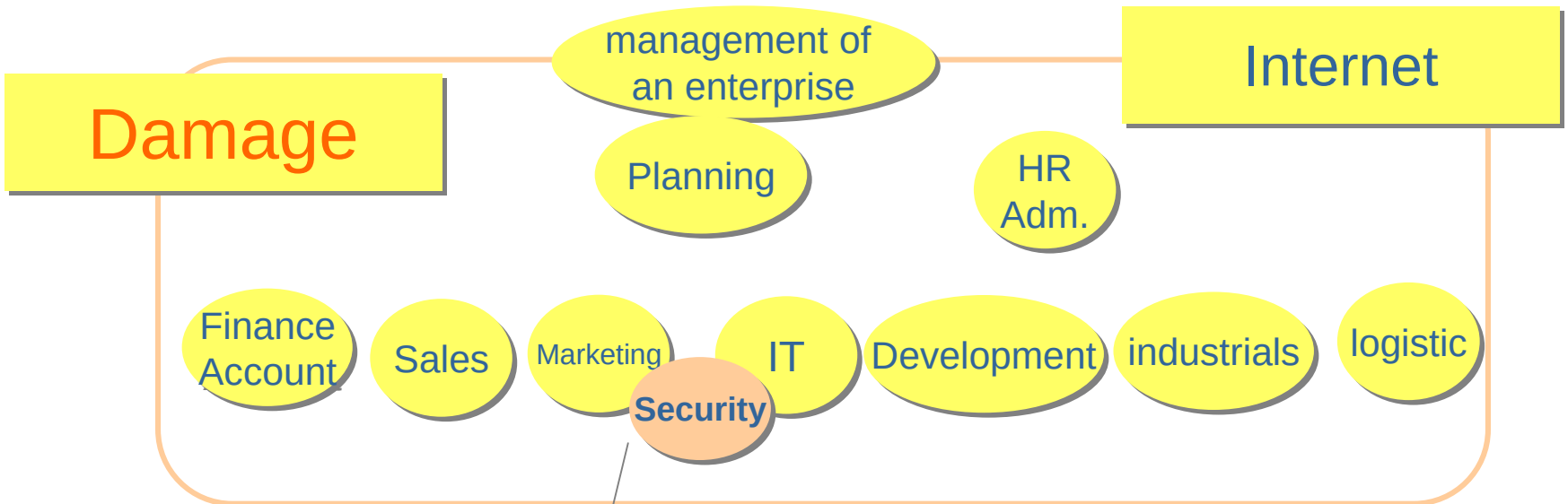
INTERNET SECURITY SYSTEMS

Changes in the position of Security

INTERNET SECURITY SYSTEMS®

Information Security in the Small Enterprise （or traditional Information Security)

A particular kind of IT(narrowly-defined Security)

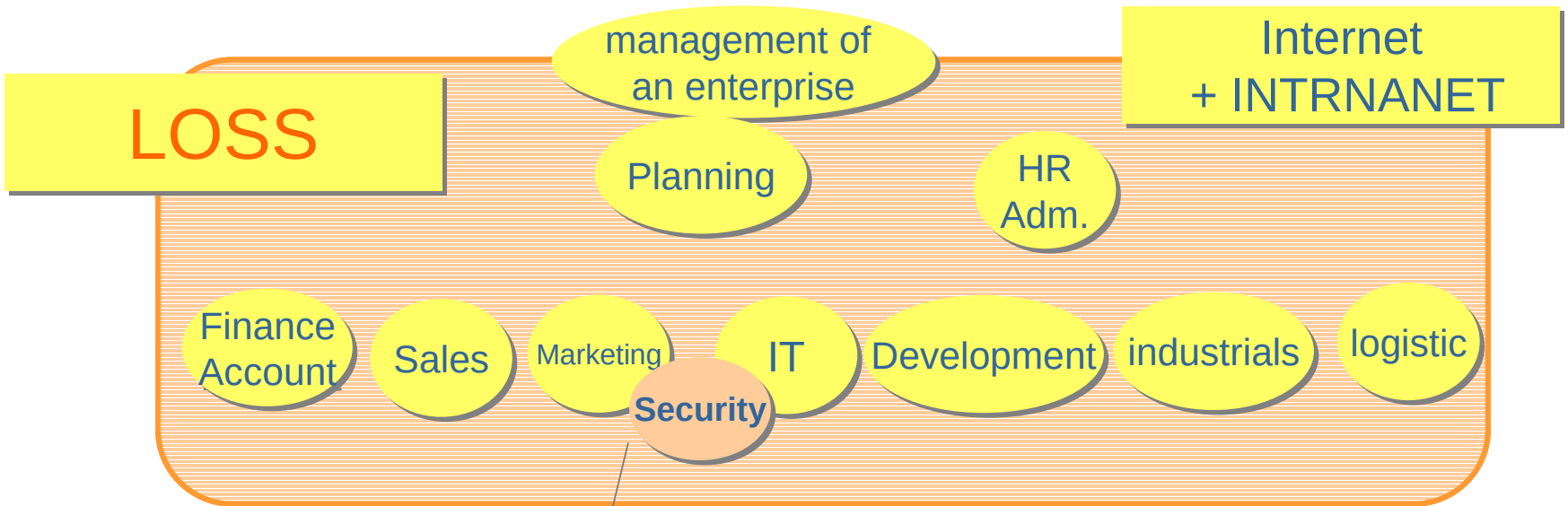


Information Security ≒ Site Security

INTERNET SECURITY SYSTEMS

Information Security in the Large Enterprise （or Current Information Security)

A part of enterprise management (widely-defined Security)



Site Security still required, but…

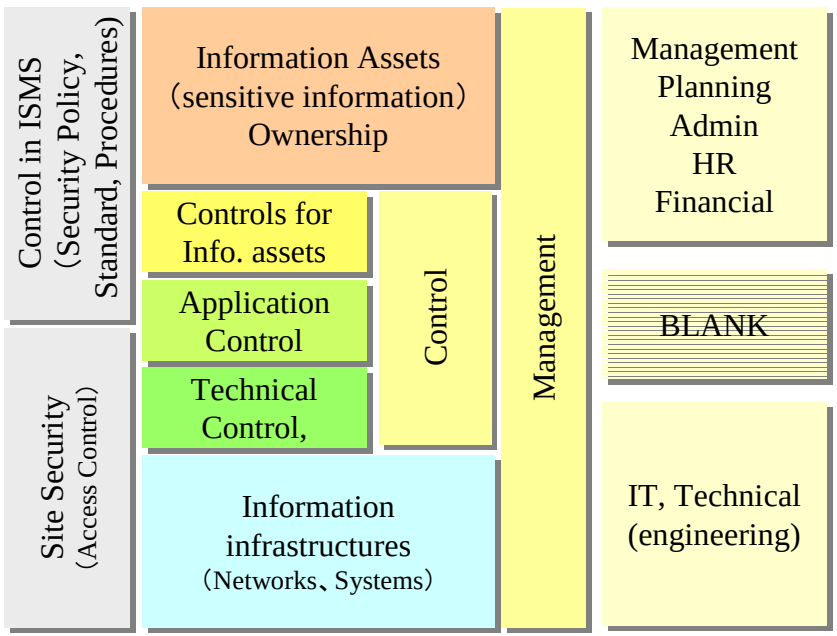
- Created ”CISO”
- Cost and benefit (SROI)
- ISMS

- ERP、CRM、。。。。
- Divulgation

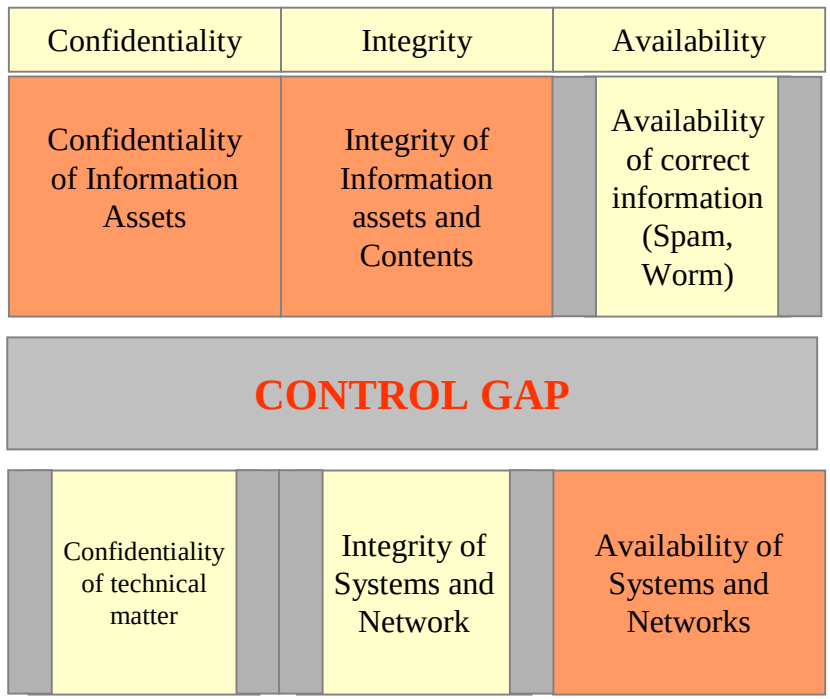
INTERNET SECURITY SYSTEMS

Widely-defined Security realized “Control Gap” in Large-Scale LAN

Widely-defined Security realize CONTROL GAPS between Security Management and Site Security, in Large-Scale LAN.



Security acts and roles



Roles and interests

INTERNET SECURITY SYSTEMS

- What to protect? Where to start?
  We'll begin with some case studies...

INTERNET SECURITY SYSTEMS®

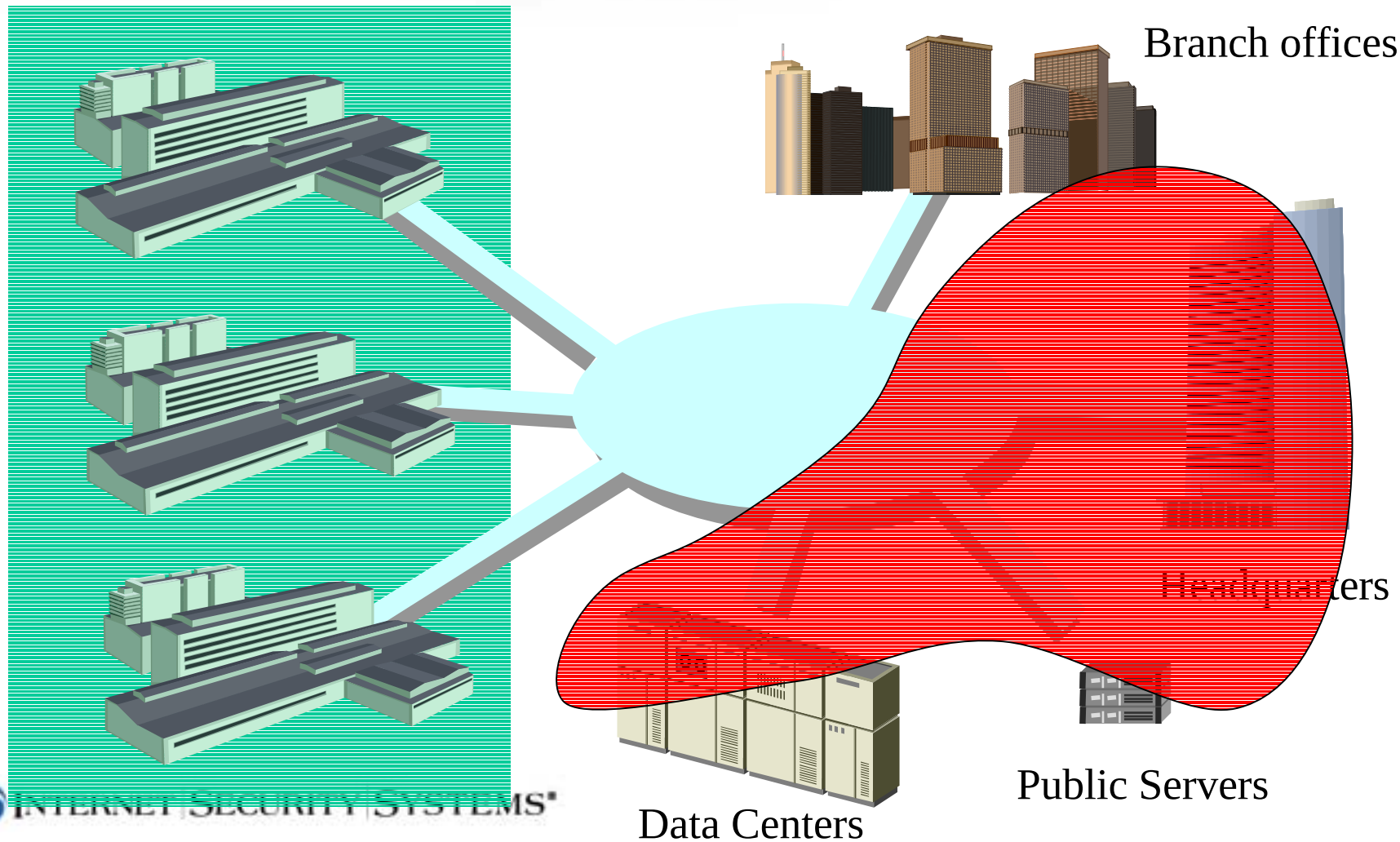
Production line
interrupted by Worm outbreak

INTERNET SECURITY SYSTEMS

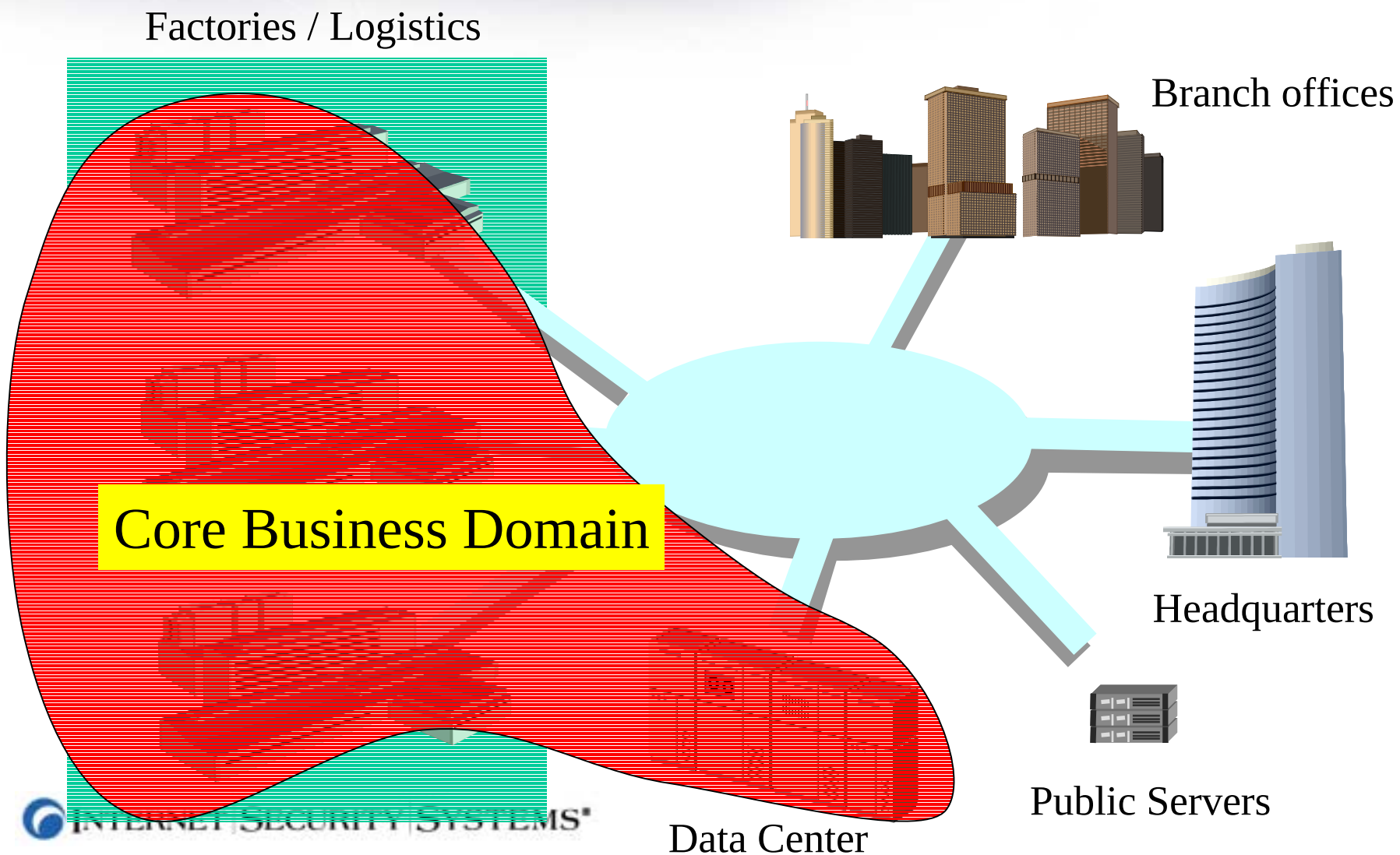
Case of a manufacturing company

- Production line was brought to a halt by Worm traffic
  - No Computers were infected in the production line.
  - But worm traffic caused a critical switch to stop functioning, resulting in a stoppage of the production line.

Typical Critical point



Actual Critical points identified after the worm incident



Personal Data loss

INTERNET SECURITY SYSTEMS

Published Leakage of Personal information

■ Recent incidents of Personal Data loss

Date	Company	Verified Losses	Type of data	Value (yen)	Notes
Mar-04	ACCA Networks	201(1,400K)	Address, name, phone number, e-mail address	0	
Mar-04	Japan Net Takata	148(660K)	Address, name, phone number, birthdate	0	
Jan-04	SoftBank BB	4,517K	Address, name, phone number, e-mail address, start of service date	500	Gift Certificate
Jan-04	ACCS	4(1,200)	Address, name, age, occupation, request content	0	
Dec-03	Tobu Railways	(132K)	Address, name, etc.	5,000	Gift Certificate
Nov-03	Family Mart	535(183K)	Address, name, phone number, etc	1,000	Quo Card
Aug-03	Aplus	79K	Address, name, housing type, salary class, etc.	0	
Jun-03	Lawson	560K	Address, name, phone number, birthdate, sex	500	Gift Certificate

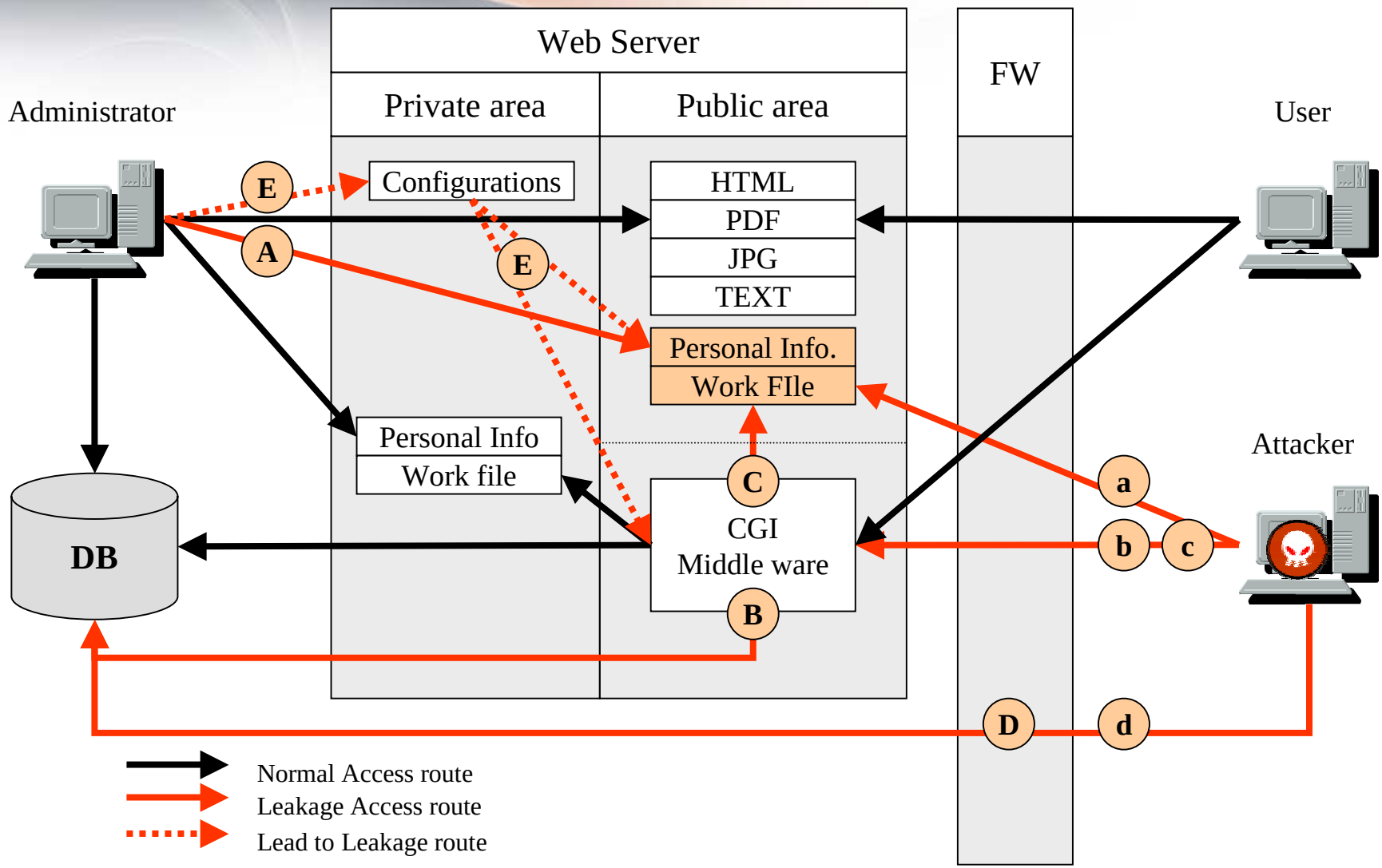
日経IT Pro 相次ぐ個人情報漏えいを振り返る　　http://itpro.nikkeibp.co.jp/free/ITPro/Security/20040329/1/

■ Legal precedent for Personal Data loss

Uji City	218K	Address, Name, Sex, Birthdate, Date of entry, Date of exit, Head of Household, Relation to Head of Household	15,000
Waseda Univ.	1,400	Names of participants	10,000
KOMMY	50K(70K)	Address, Name, Birthdate, Phone number, Personal information	50,000
KDDI	9K(32K)	Phone number, address, name, call history	1,000,000

INTERNET SECURITY SYSTEMS

Typical Leakage routes

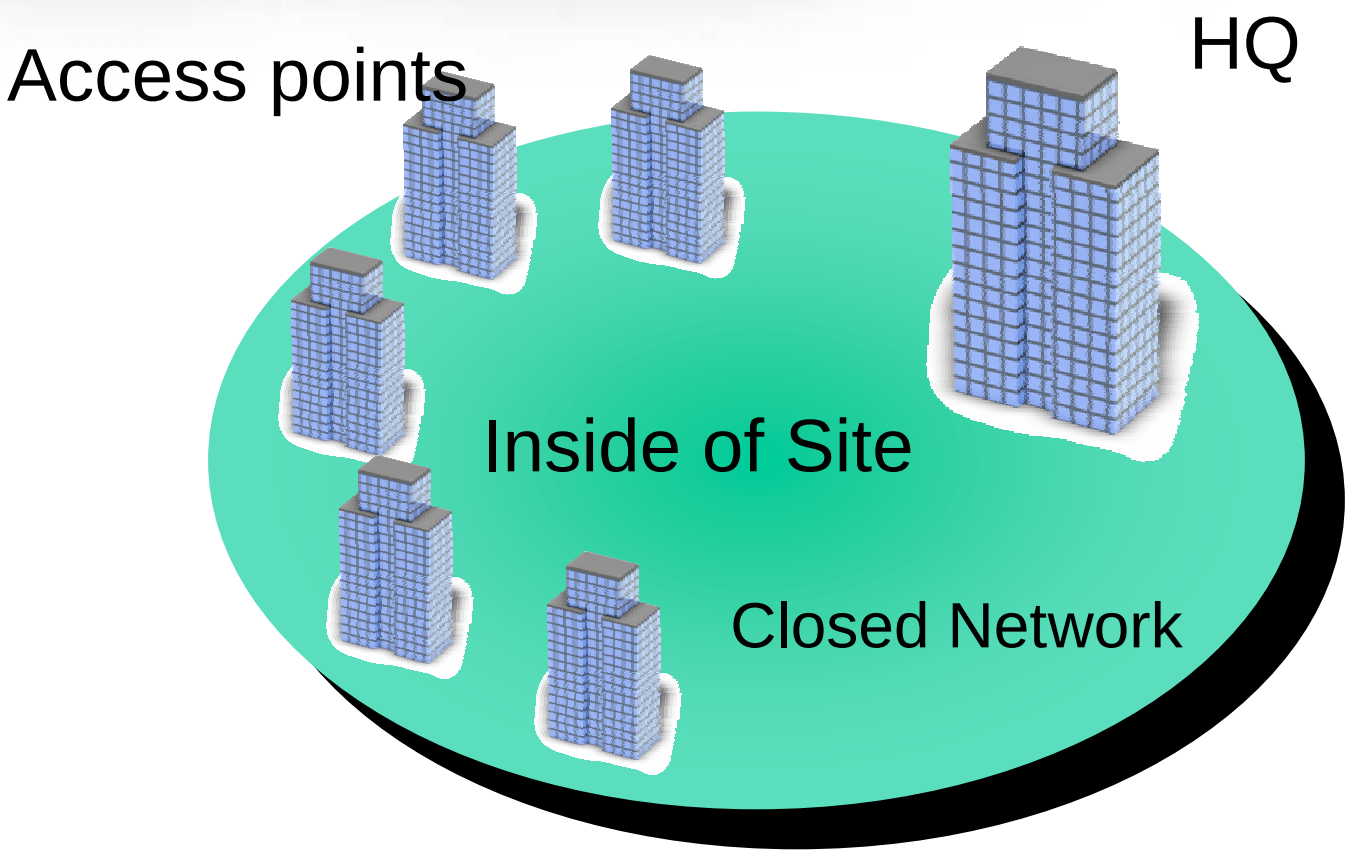


INTERNET SECURITY SYSTEMS

Information Security Overview

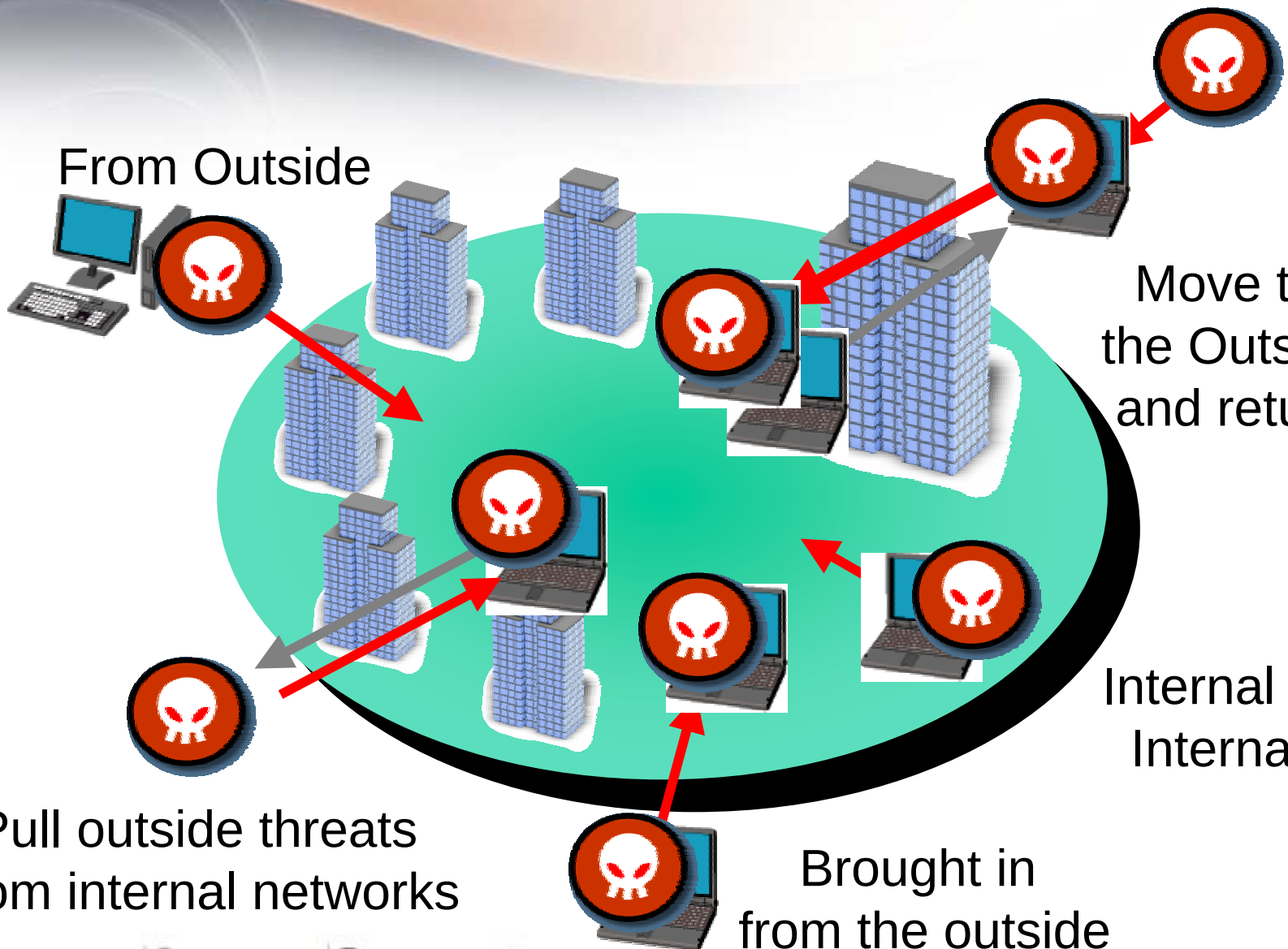
INTERNET SECURITY SYSTEMS®

Direction of threats



INTERNET SECURITY SYSTEMS

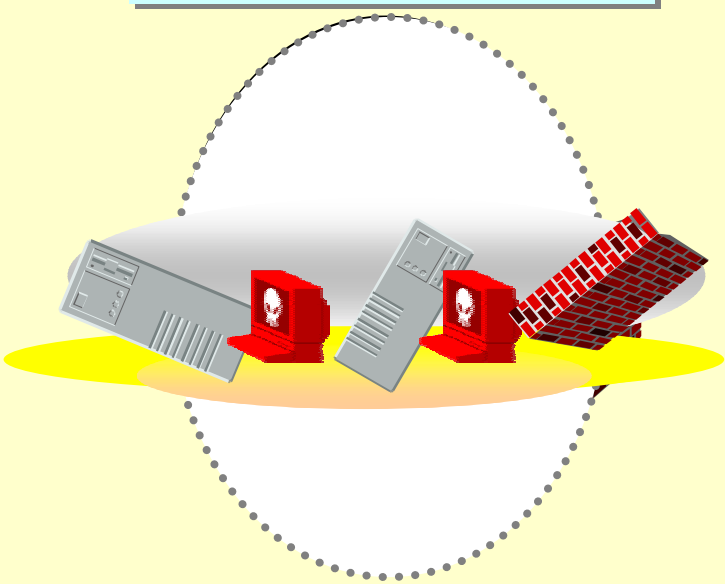
Direction of threats



INTERNET SECURITY SYSTEMS

Practical Limit to Point Solutions

Practical limit to point solutions

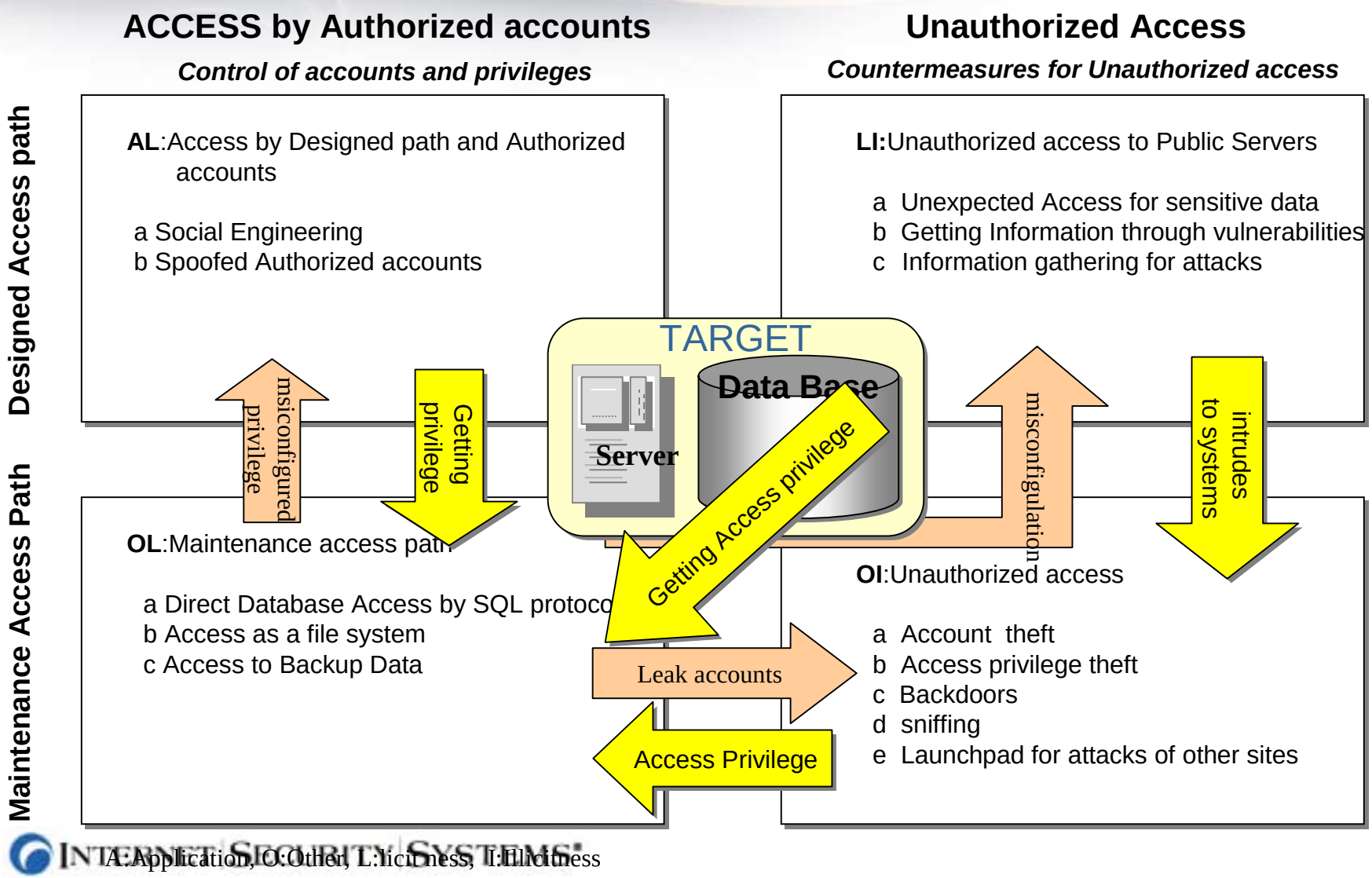


Affected PCs brought in
Affected PCs attack internal network
Direct connection via Wireless LAN

Image of total information security

Affected PCs brought in
Affected PCs attack internal network
Direct connection via Wireless LAN

Routes of Unauthorized Access



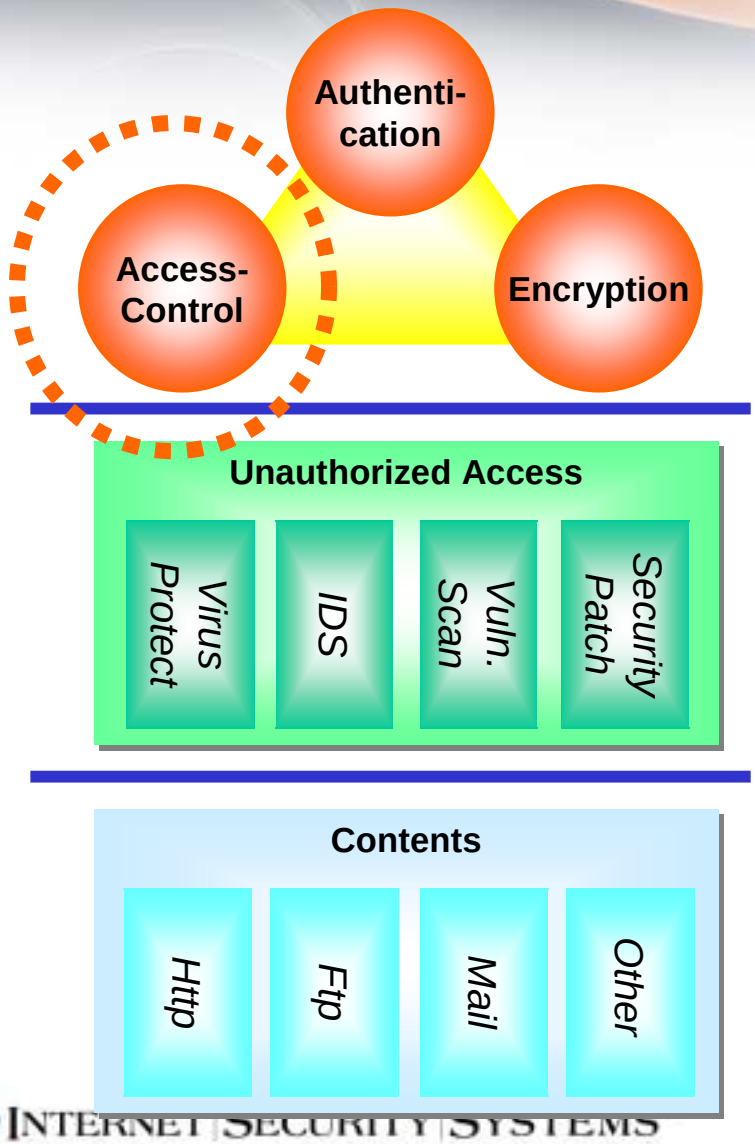
A:Application, O:Other, L:licitness, I:Illicitness

Countermeasures to Unauthorized Access

INTERNET SECURITY SYSTEMS

Typical Countermeasures

Network Security Layer



Basic Security Layer(CIA)

Control users, services, confidentiality by Authentication, Access Control, Encryption

Exploit Protection Layer

Detect and eliminate packets which may impact services
（virus、Worm、DoS、Backdoor, etc）

Content Security Layer

Detect and eliminate unwanted content
（Sexual data, privacies, critical information ）

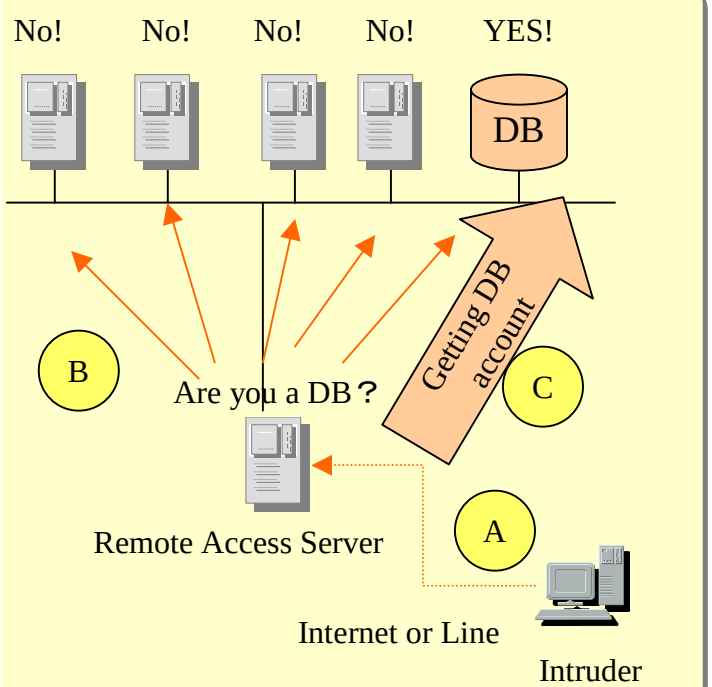
INTERNET SECURITY SYSTEMS

Work of Segmentation and perimeter protection

INTERNET SECURITY SYSTEMS

Estimation of efficacy of access control

A case of leakage



Estimation

Week ACL

1.4 times	100%	100%
1.4 times /Year	1.4 times /Year	1.4 times /Year
A:Network	B:DB Probe	C:DB Account Crack → D: Information abuse
0.14 times /Year	5%	1%
1.4 times/10years	1.4 times/200years	1.4times /20000year

Well Controlled ACL

Estimate from "theft crime rate" in Japan (Average of 1996-2000)

http://www.police.pref.saitama.jp/kenkei/koho/kohosiryo/hakusyo/zisyo/zisyo/z1.html

INTERNET SECURITY SYSTEMS

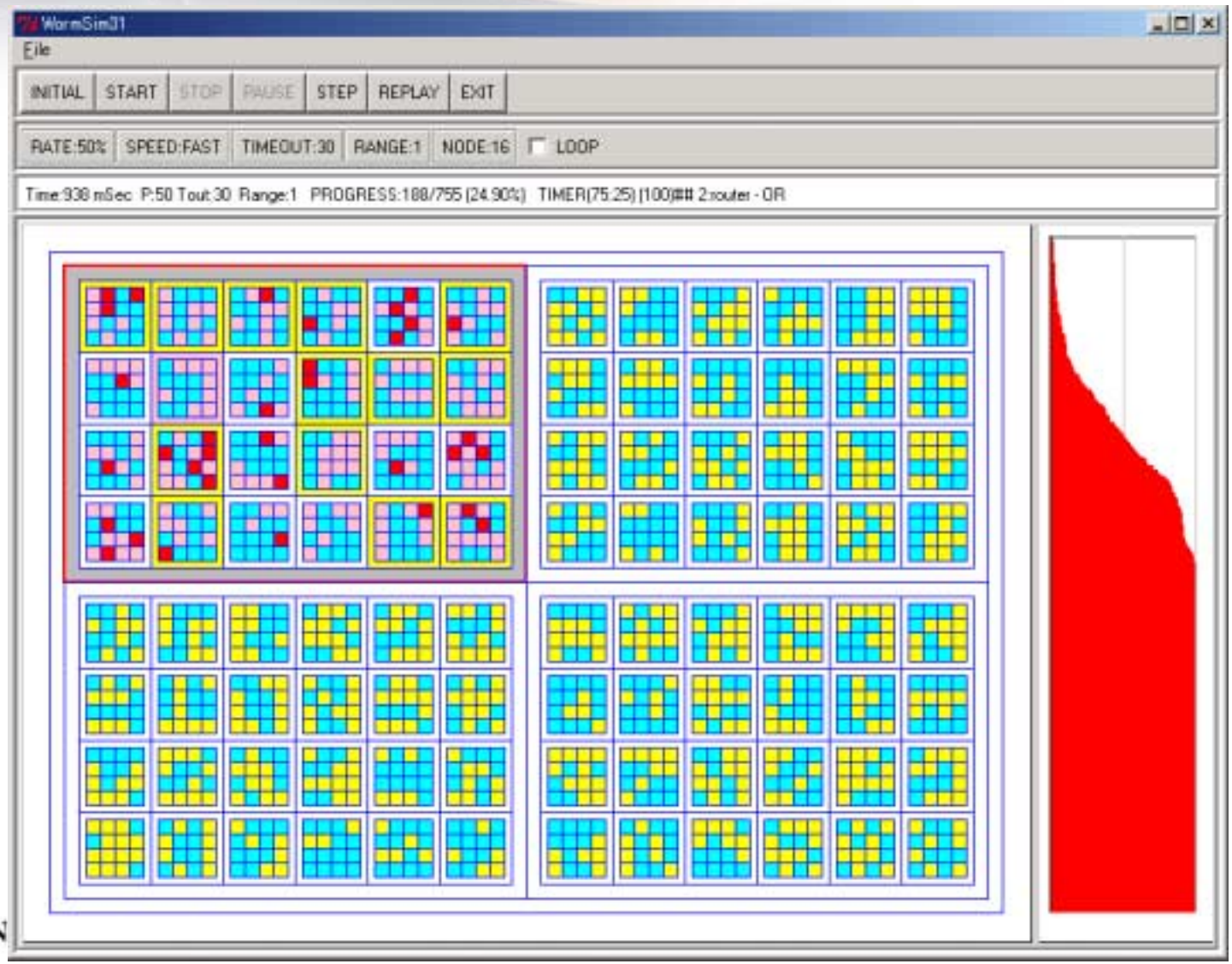
Countermeasures for Virus and Worms by ACL

- ACLs prevent much virus and worm activity
  - Outbound access control
    - In many cases, even sites that manage Inbound traffic neglect Outbound traffic.
    - Controlling outbound traffic prevents many viruses and worms from spreading
    - For example,
      - Dropping Port 25/TCP can prevent mass mails by viruses
      - In Many cases, Spyware and Phishing software uses High TCP ports
  - IPS is effective for viruses and worms
    - Inline IDS (IPS) is now fit for practical use

ACL Drop or Reject?

- There are two main methods to block traffic by Access Control
  - DROP and REJECT
  - See the result of worm propagation under Drop policy and Reject policy

Worm propagation under Reject policy



Worm propagation under Drop policy

Worm propagation

*Worm propagation under "**RESET**" policy*

*Worm propagation under "**DROP**" policy*

INTERNET SECURITY SYSTEMS®

- Problems which cannot be solved by using ACLs

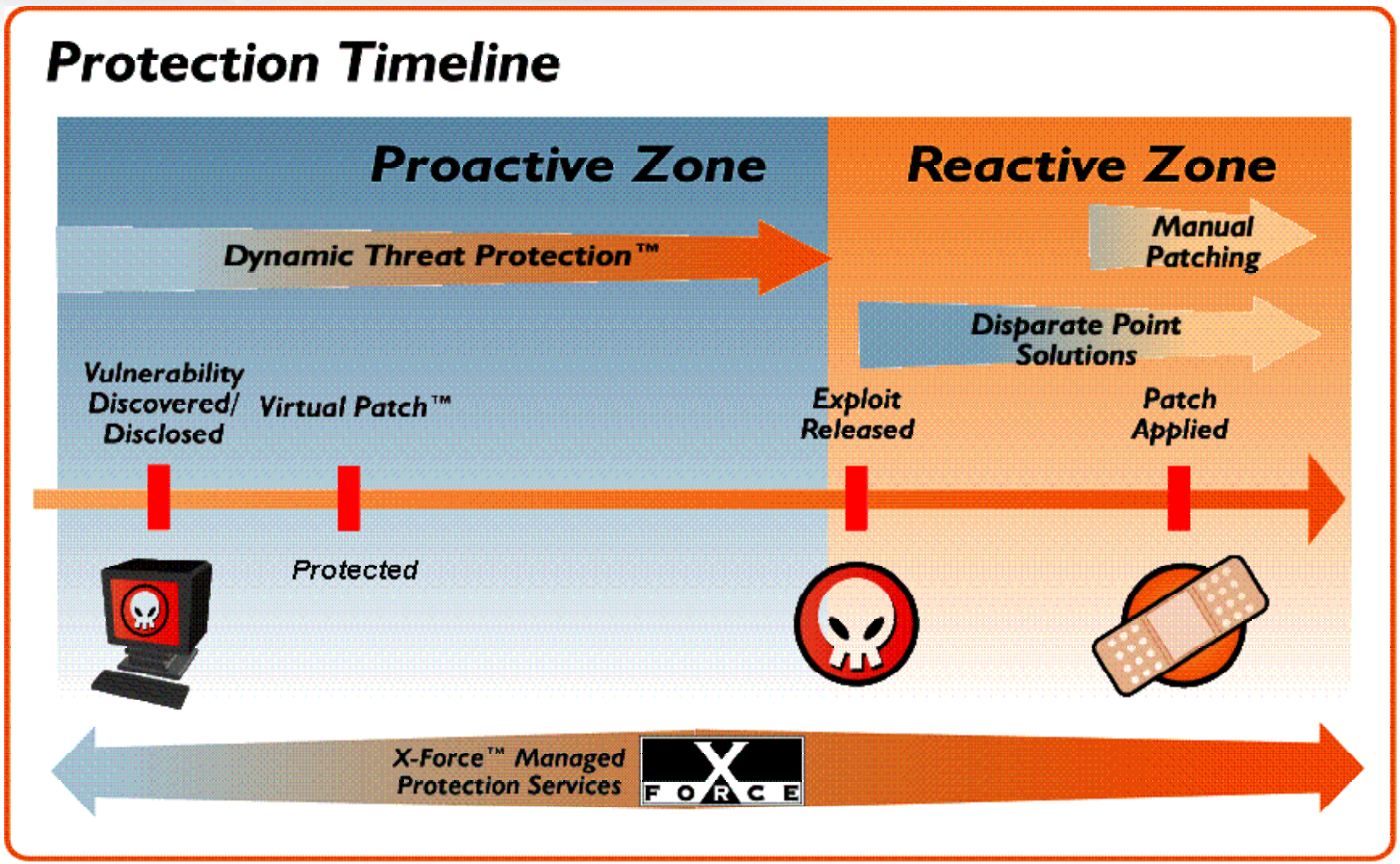
Malicious packets which bypass ACLs

- How to prevent attacks/packets which avoid ACLs
  - Basically, fortify endpoints, but…
    - It is difficult to Control all nodes
    - Patching systems takes time
  - Alternatives
    - Perimeter prevention using IPS technology
    - Cell protection by Personal Firewall

→ Let's see …

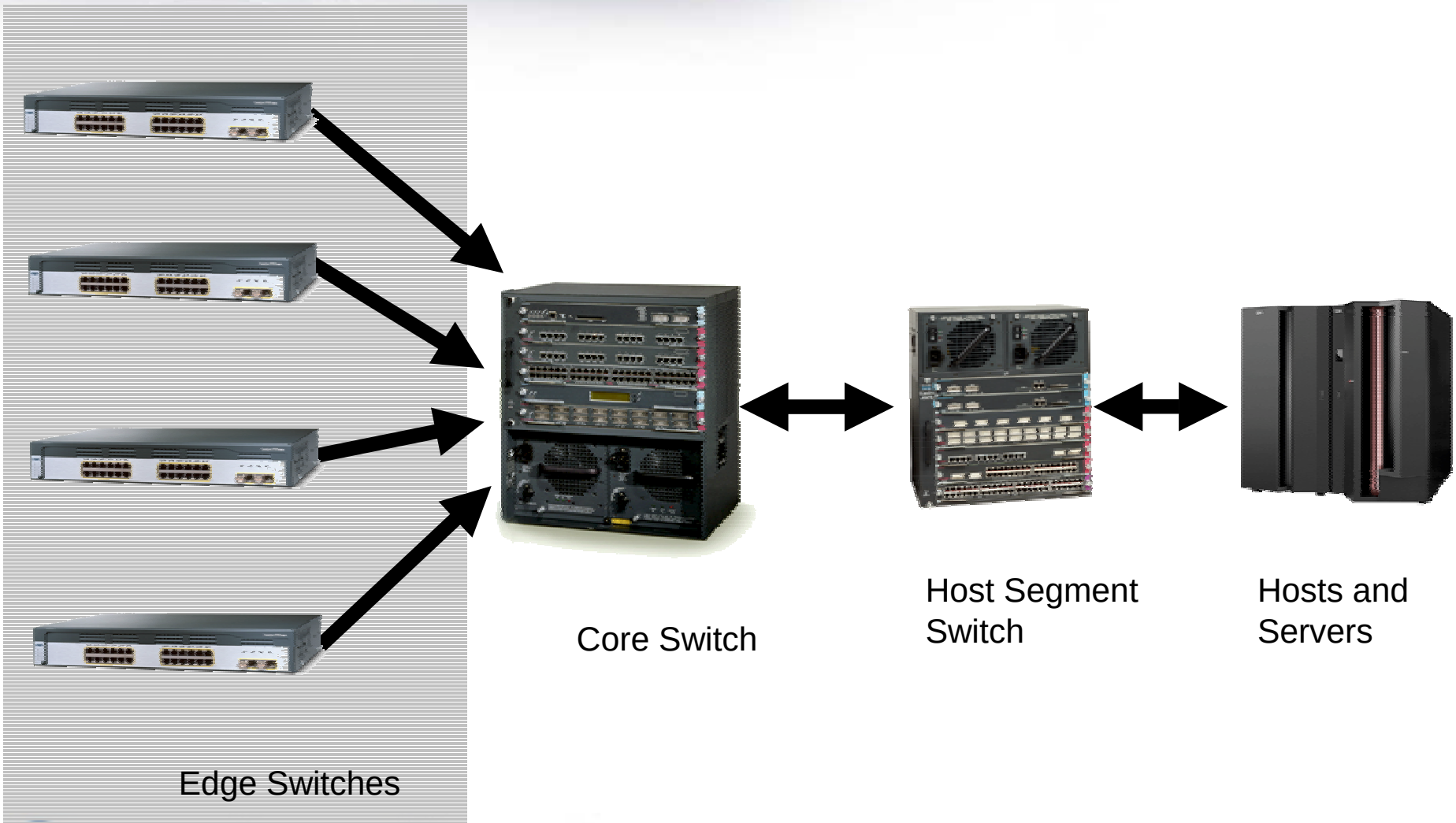
- Vulnerability life cycle
- Segment prevention examples, with a focus on availability.

Lifecycle of Vulnerabilities



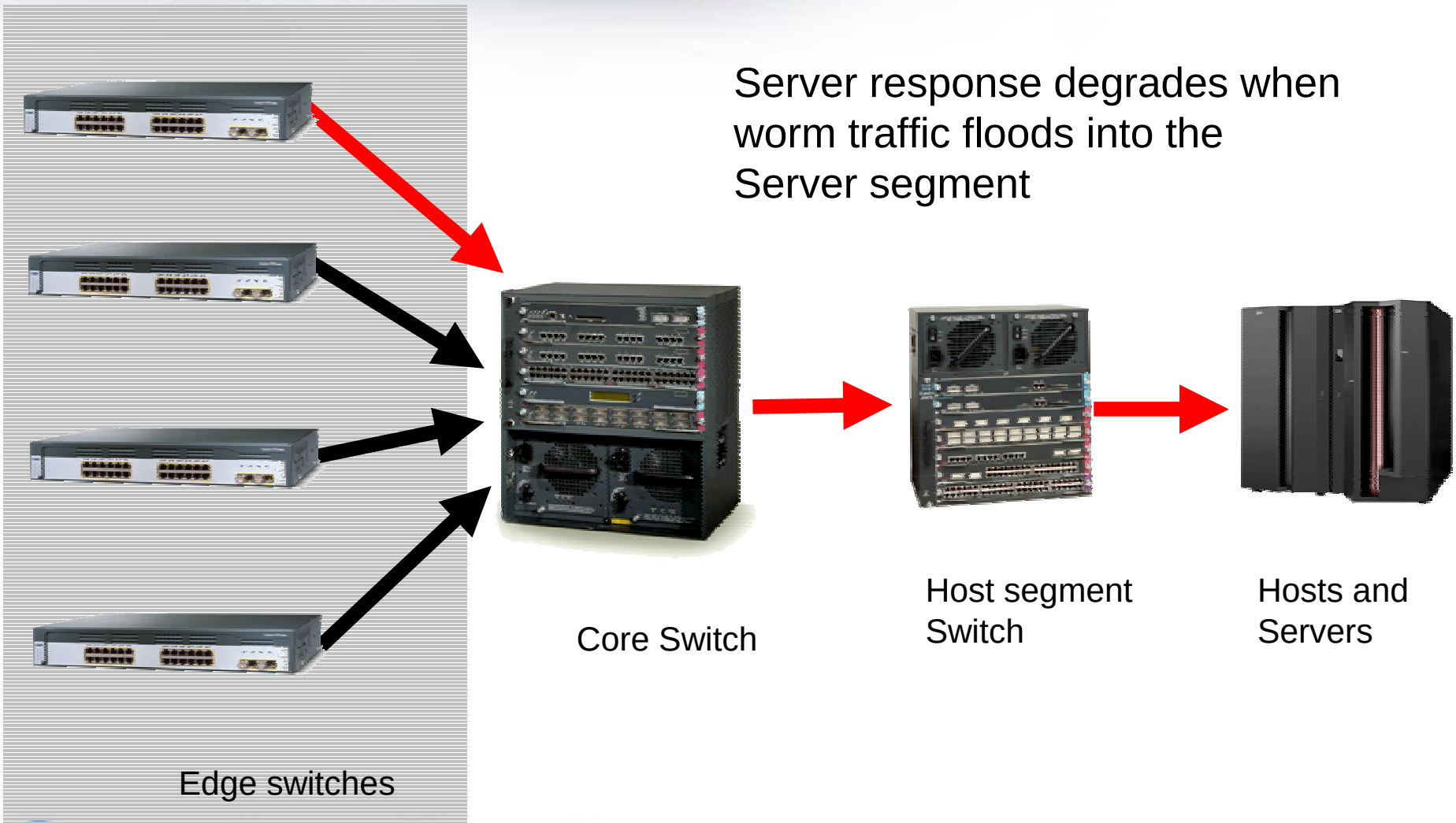
INTERNET SECURITY SYSTEMS®

Low availability caused by worm traffic



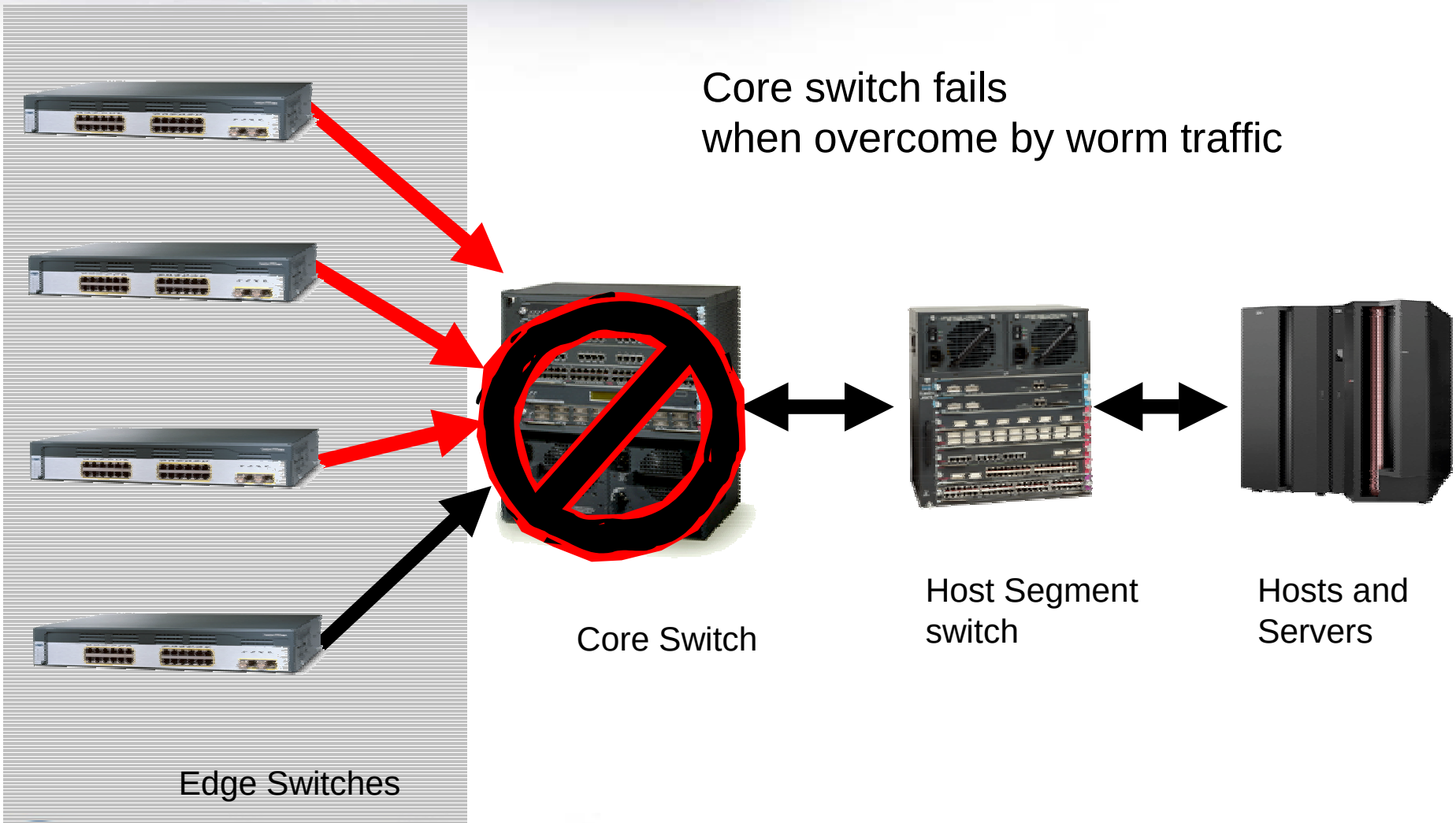
INTERNET SECURITY SYSTEMS

Low availability caused by worm traffic Pattern-1



INTERNET SECURITY SYSTEMS

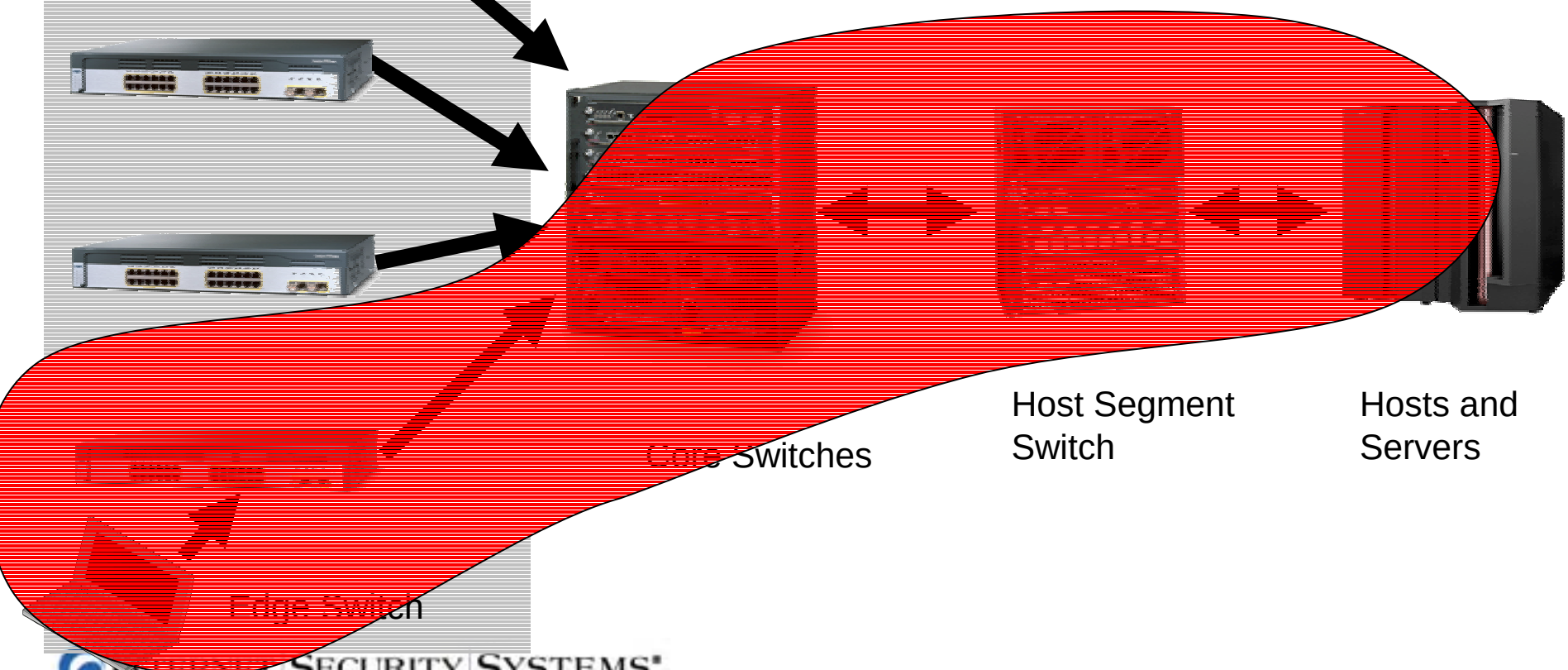
Low availability caused by worm traffic Pattern-2



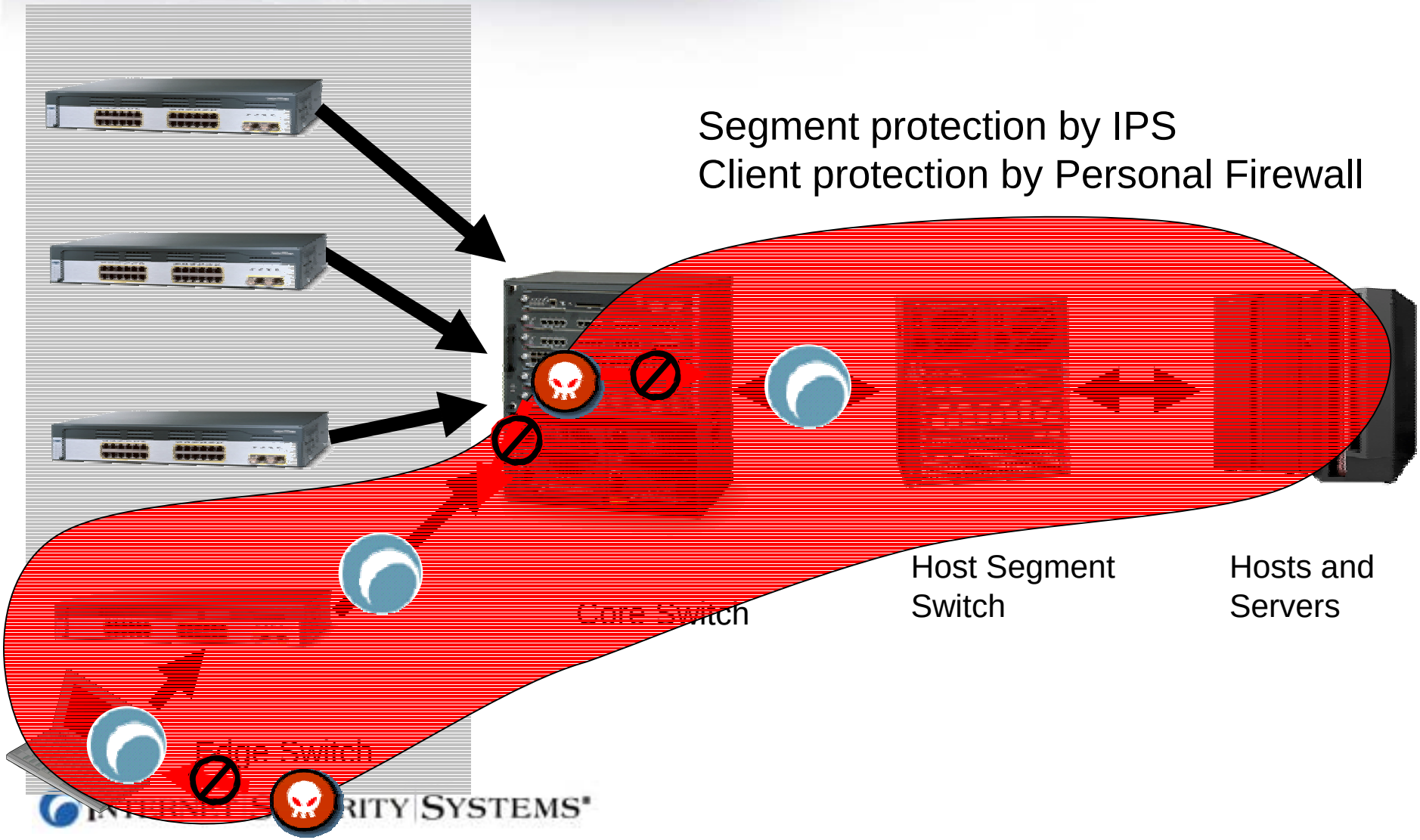
INTERNET SECURITY SYSTEMS

Improving availability

Need to protect the “access path” between clients and servers

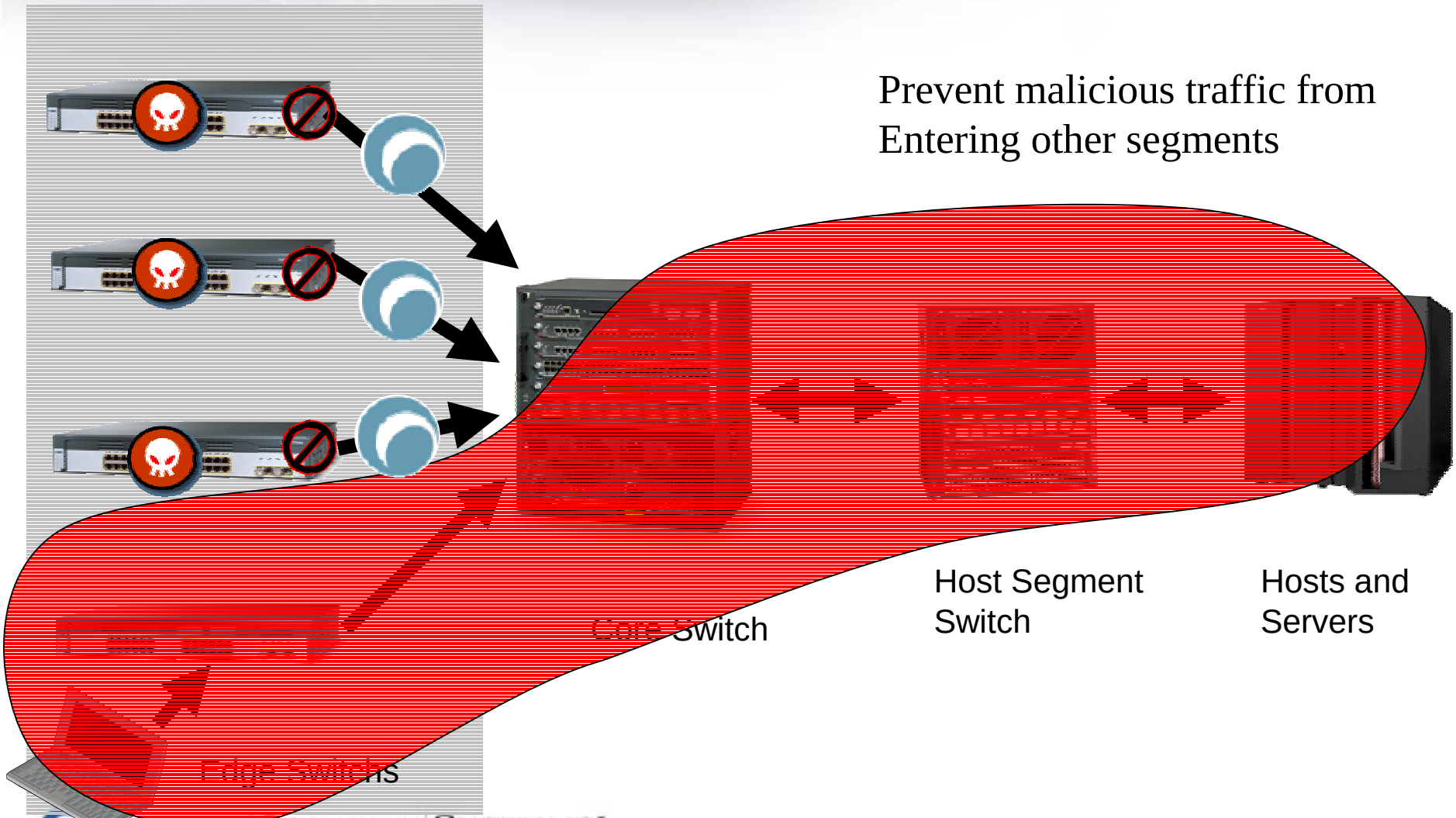


Protect the Access Path



Sealed traffic

Prevent malicious traffic from
Entering other segments



INTERNET SECURITY SYSTEMS

Typical misconfigurations
found during Security Auditing

INTERNET SECURITY SYSTEMS®

Accounts and Passwords

- Account Management
  - Prevalence of weak passwords
    - Blank Password（ex. Administrator on PDC was blank)
    - Default Password（ex. Scott, sa, ）
    - Guessable Password（root = root, Administrator = Administrator）
  - No enforcement for safer Password
    - Password complexity, enforced mechanisms, expiration
  - Not only Servers but also…
    - Management protocols and accounts on Routers and Switches
    - HSRP Default Password（anybody can re-route）
    - SNMP Default community name
  - No enforcement for account lockout
    - Operating System, Database…

INTERNET SECURITY SYSTEMS

Basic Control – 2

- Access controls for administrative privileges
  - Services with Administrator accounts
    - Web Servers, Mail Servers, DNS Servers
    - Database and other Middleware
  - Access Control of Management Pages
    - Web-based management pages abound, but…
      - Authentication is not controlled
      - In many cases IP-based control is not implemented
- Database account controls
  - Without control here, sensitive information is extremely vulnerable
    - Non-administrative accounts have administrative access
    - Access to DB resources using OS-level accounts
    - Incorrect assignment of Resource Roles
      - Able to add clusters, procedures and triggers

Network Topology Issues– 1

- Network structure and network devices
  - Firewalls set to Accept by default
    - Only blocks certain protocols, leaves other ports open
      - SMB(NetBIOS), SQL, TFTP are allowed
        - » Worms may use these protocols to spread
      - Why is chat software necessary?
  - Too much trust placed in the firewall alone
    - Internal network security ignored
      - Did you have to deal with the likes of MS Blast or Nimda?
      - Cannot defend against attacks let through the firewall
  - Inter-segment access control not implemented
    - Any access allowed from DMZ to any segments
  - Routers and Switches not protected
    - Telnet allowed to external interfaces of border hardware
    - Accounts and passwords still set to default values

Network Topology Issues – 2

- Server settings
  - Unnecessary services running
    - Especially, servers installed without the knowledge of security staff
  - Logging not enabled
    - Especially Windows servers
  - Unnecessary features enabled
    - Webserver modules, dynamic objects
  - Use of Rlogin, .rhost settings
    - “+” in the /etc/hosts.equiv file
    - Presence of ~/.rhost files
  - Permissions
    - Logs and /etc are world-writable
  - Patches not applied

Operational Issues

- Security Patches
  - Patching is not included in operational planning
    - Because patching is unplanned, it does not occur
    - Production servers are patched without testing (Windows Update)
- Backup
  - Is the backup plan appropriate?
    - Backups are not taken properly
    - Lack of experience restoring from backups
      - Unknown whether backups are being taken
      - Unknown whether backups are restorable
    - Has an appropriate backup medium been decided upon?
  - Is there a clear recovery plan?
    - How long will recovery take? 1 hour? 1 week?
- No emergency procedures in place
  - How to find the problem? Who handles it?
  - Who knows the escalation path?

Lack of knowledge regarding current status

- Unknown IPs and ports
  - Results of security evaluations
    - Discovery of unused IPs active on the network
    - Discovery of supposedly unused services (ports)
- Network topology
  - In how many minutes can the following information be retrieved:
    - Full network diagram and firewall rule list
    - List of active servers by OS
- “Normal” state of the network is unknown
  - We’re being DDoSsed! Help!
  - The network seems slow… I wonder why…
  - Does the network administrator realize the extent to which chat, p2p, webmail, etc. are in use on the network?

Other issues -1

- AV software updates
  - Updates done, but by hand (not automatic)

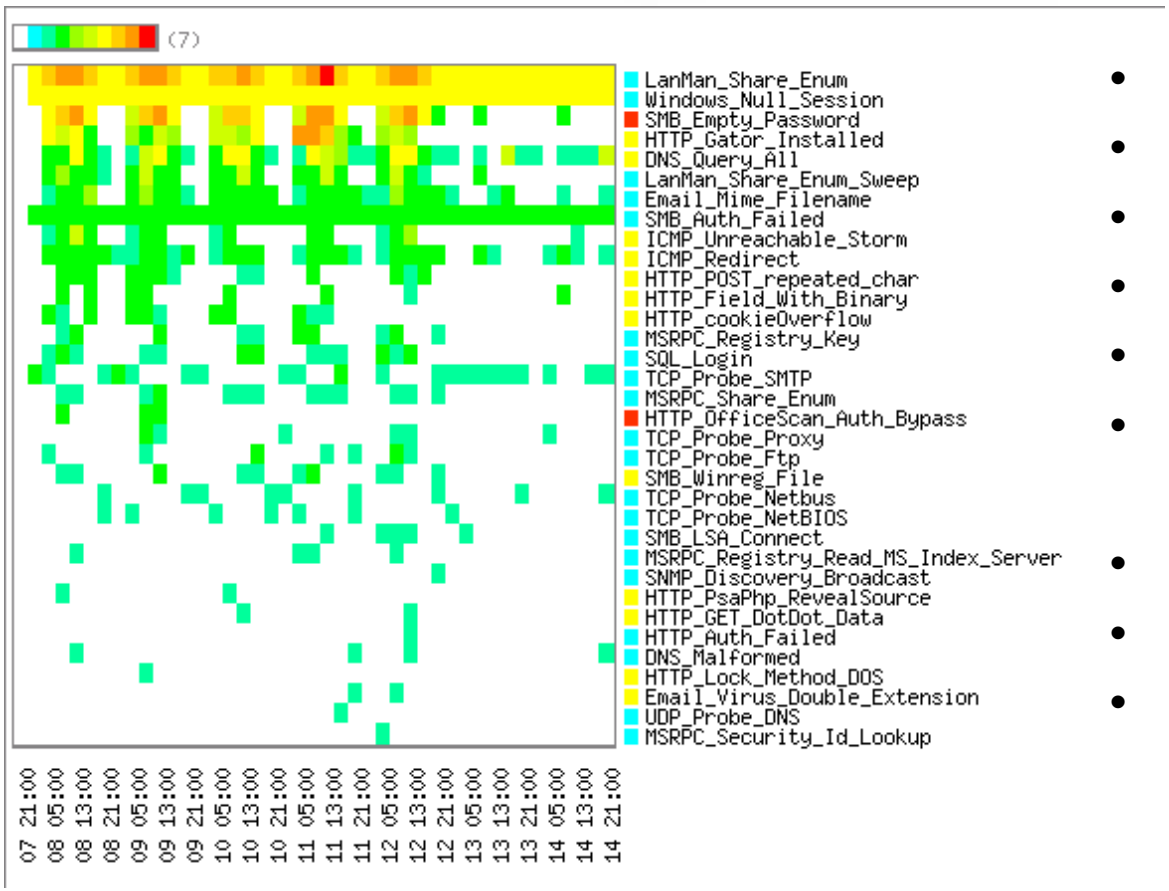
- Personal, educational, administrative problems
  - While watching the server room, senior employees come and go
  - They accidentally shut down the server with blank passwords
  - At that point, I should have said, “You need to define a password.”
    - One senior lady told me with a smile,

    - “I can’t remember too many passwords” ☺

Other issues -2

- Database settings
  - Passwords used by automated processes are hardcoded
    - For example, xxx = abc
  - Delegated permissions are not granular
    - Any account has write permissions
  - IPs from which SQL queries can be sent are not restricted
    - A problem in many organizations
- Mailserver settings
  - 3rd-party relay is important, but so is setting limits
    - There are users sending large files over e-mail
    - The mail sent, but after awhile an error was returned
      - Receiving server may have been brought down
    - When they receive an error, they resend the message, and now the local mailserver can't handle the strain…

Example of Actual Network



- Blank passwords
- Weak passwords
- Authentication failures
- SQL connections
- Virus traffic
- SQL Injection

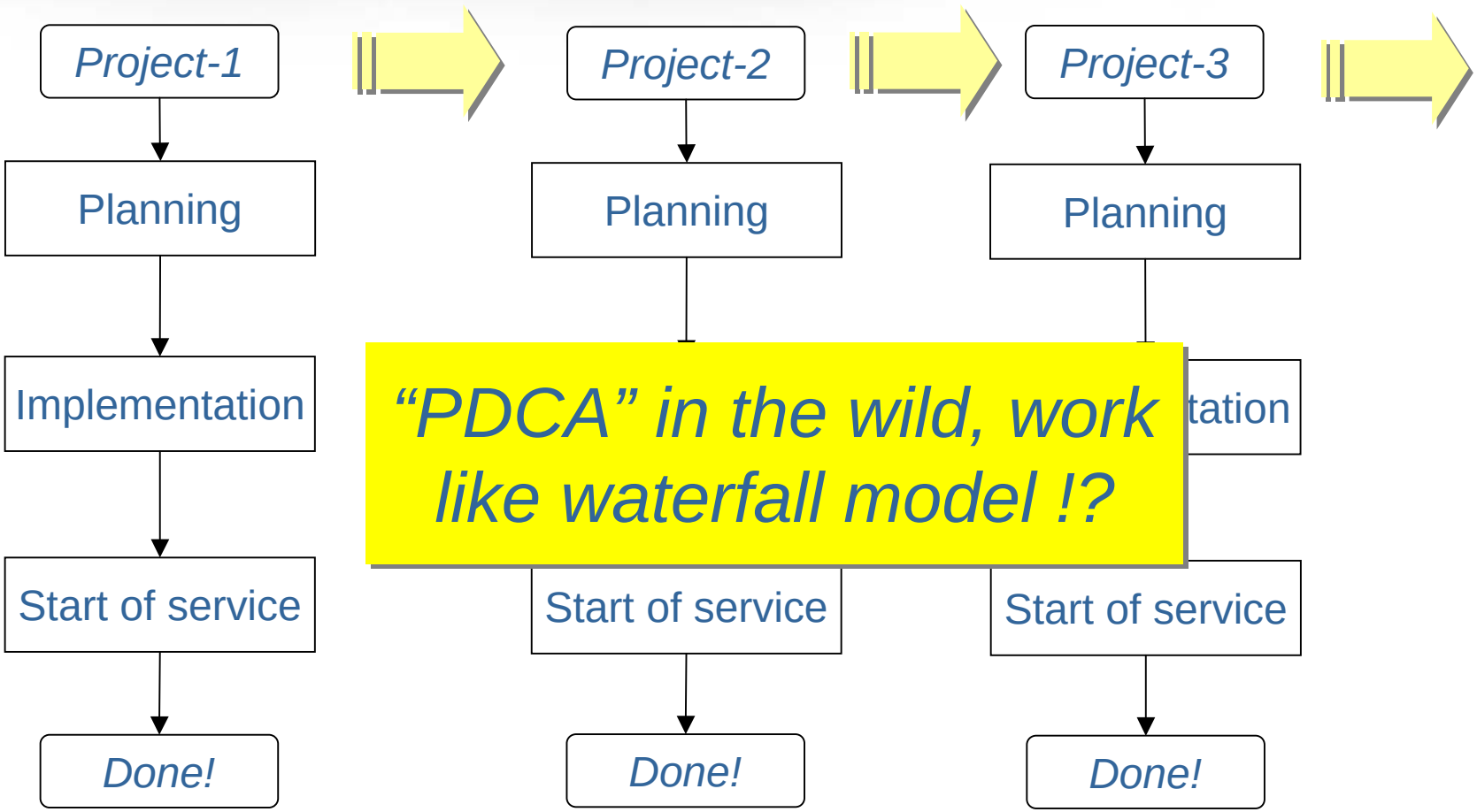
- Chat(IRC)
- Web Mail
- IPv6

INTERNET SECURITY SYSTEMS

Operations and ongoing risk management for Large-Scale LAN

INTERNET SECURITY SYSTEMS

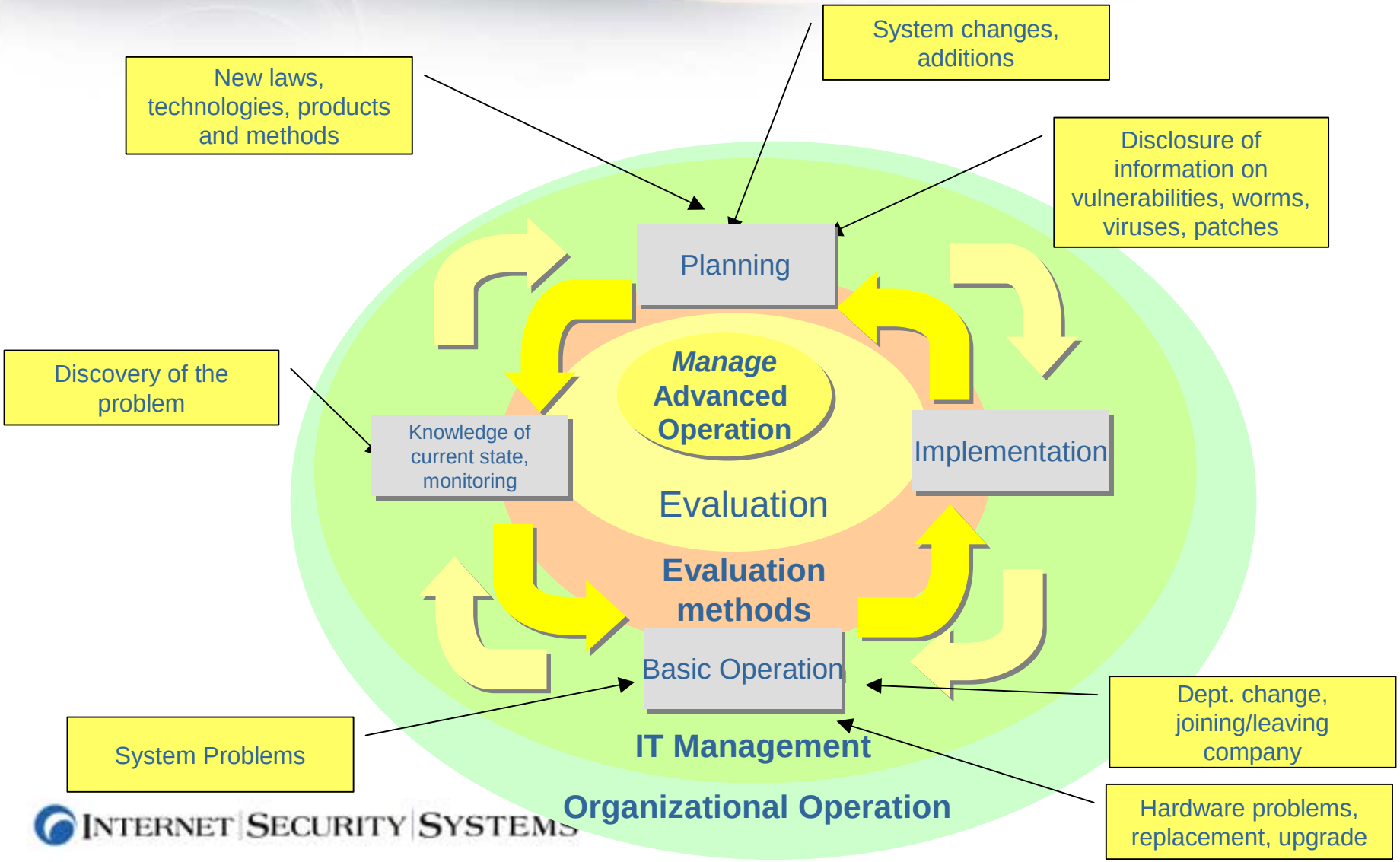
Typical Procedure for Security implementation
The waterfall model



INTERNET SECURITY SYSTEMS

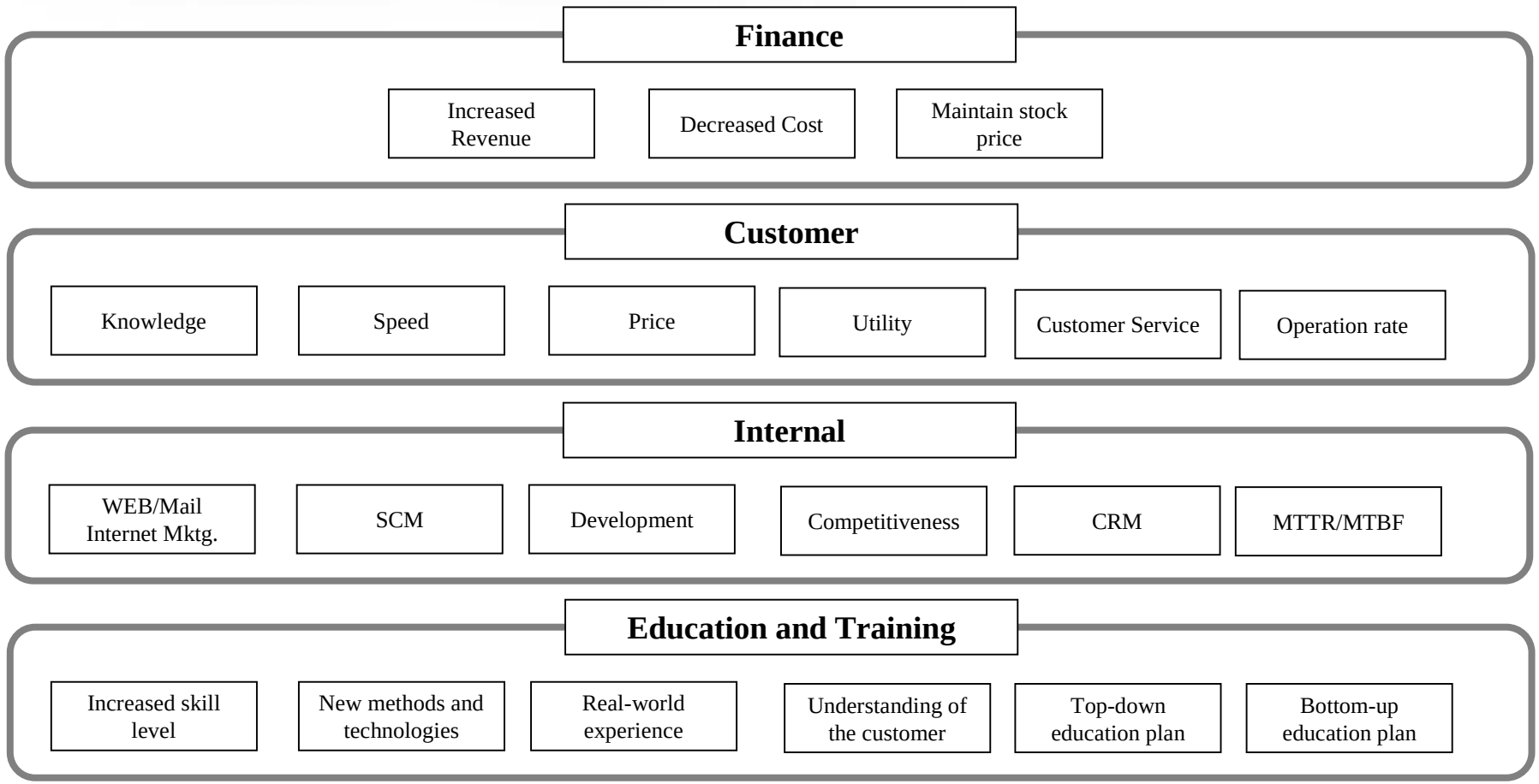
Advisable Procedure for Security implementation

PDCA + α



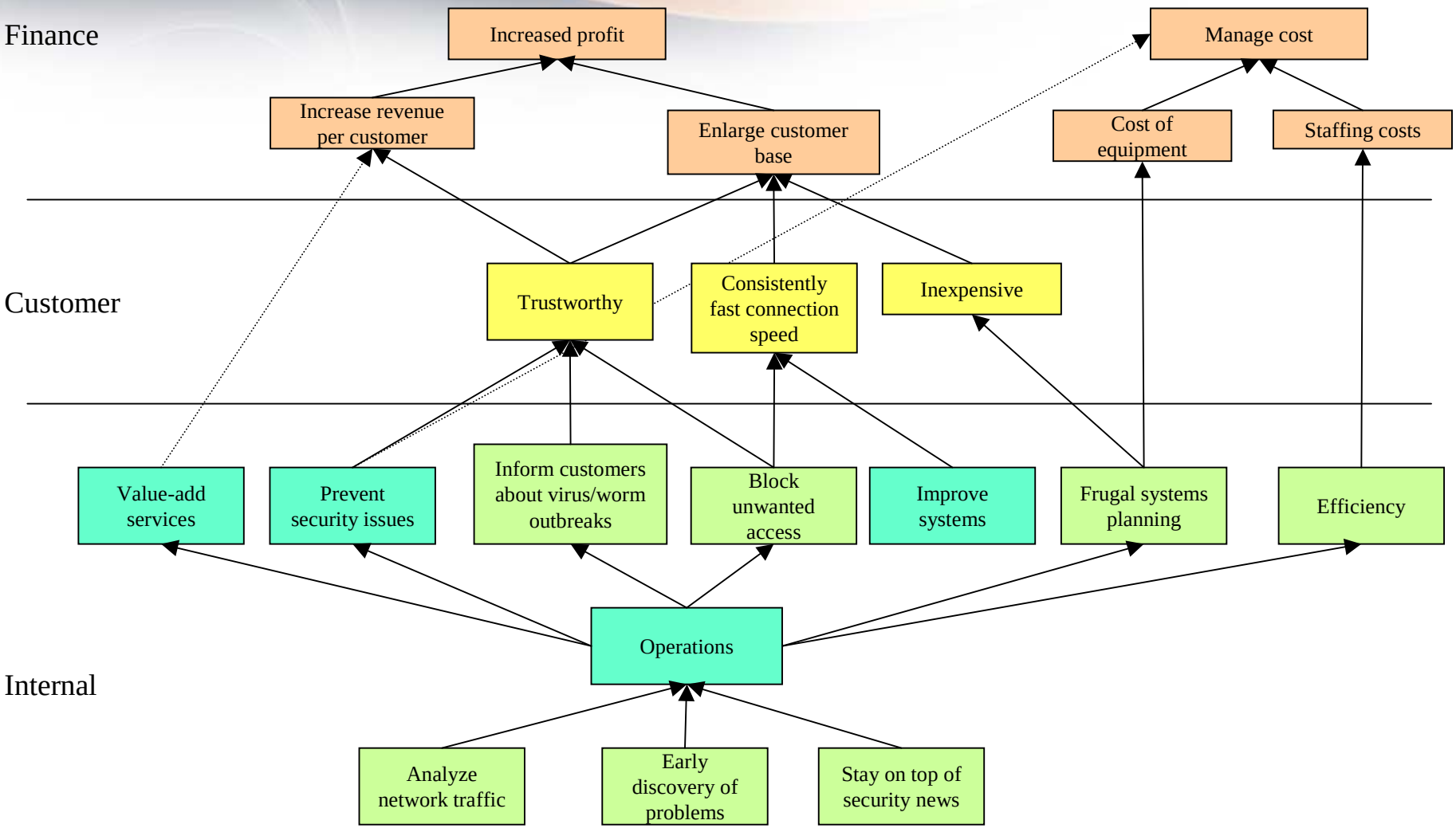
INTERNET SECURITY SYSTEMS

When the PDCA cycle is difficult to evaluate: The BSC (Balanced Score Card) Approach



INTERNET SECURITY SYSTEMS

Example of simple BSC for ISP



学習と成長の視点

In summary

INTERNET SECURITY SYSTEMS

In summary

- Security for Large-Scale LAN Design,
  - Technical Point
    - Perimeter protection（Outbound + Inbound)
    - Node(cell) level protection（Hardening and Personal Firewall）
    - Preparing quick response measure（IPS, Virtual Patch）
      - It takes time and energy for large-scale LANs
    - Knowledge of current state(monitoring)
      - Understand the Normal state
      - Watch for attacks and anomalies
  - Specific point for Large-Scale LAN
    - Read for consistency with Enterprise management
    - Protect the core business domains
    - Follow PDCA+α Model instead of discontinuitive waterfall model
      - Especially, implementing evaluation is important.
        - » BSC or other management method may be useful

INTERNET SECURITY SYSTEMS

Thank you!

mtakahashi@isskk.co.jp

INTERNET SECURITY SYSTEMS