The Small Business Security Workbook

Susan Lincke PhD CISA
Assoc Prof Computer Science
University of Wisconsin-Parkside

Acknowledgments

Material is from:

- CISA Review Manual, 2009
- CISM Review Manual, 2009
- All-in-One CISSP Exam Guide, 4th Edition, McGraw Hill, 2008
- Essentials of Corporate Fraud, T L Coenen, John Wiley & Sons, 2008
- The Art of the Steal, Frank Abignale, Broadway Books, 2001

Author: **Susan J Lincke, PhD CISA**
Univ. of Wisconsin-Parkside
Contributors: Gabriel John, Tim Dorr, Todd Burri
Reviewers: Tim Knautz, Will Zheng

Funded by **National Science Foundation (NSF)** Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and/or source(s) and do not necessarily reflect the views of the National Science Foundation.

Small & Medium Businesses (SMB)

- Can employ up to 500 employees
- Make up 95% of all business in the U.S.
- Produce about 50% of our GNP
- Employ about 50% of employees [NIST]

In Europe, a Small and Medium Enterprise (SME):

- employs less than 250 people
- makes up a large portion of businesses

Research shows that SMBs/SMEs:

- Lack security – lack time, expertise, $$
- Lack security awareness
- Not aware of security regulation

Businesses in general performed according to their size: large best, medium next best, and small worst.

Small Business Adhere to Security

- Breach Notification Law
- Payment Card Industry Data Security Standard (PCI-DSS)

Specific Industry Regulation affecting SMBs:

- HIPAA: Health Insurance Portability & Accountability Act
- FERPA: Family Education Rights & Privacy

Security Standards

General Security Standards

- ISO 27001
- FIPS (NIST)
- COBIT
- CISSP – CISA – CISM

Small Business Security

- NISTIR 7621 Small Business Information Security
- Small Business Security Workbook

Small Businesses can’t devote someone to Security

Security Workbook Objectives

- Accessibility to non-professionals
- Easy to use
- Based upon professional standards
- Full-featured
- Tailored to individual organization’s requirements
- Documented
- Useful for Educational & SMB Use
- Free

Small Business Security Workbook - Overview

3. Strategic Security Plans

- 3.1 Code of Ethics
- 3.2 Policy Manual
- 3.3 Risk Analysis
- 3.4 Business Impact Analysis & Business Continuity

4. Tactical Security Planning

- 4.1 Information Security
- 4.2 Network Security Plan
- 4.3 Physical Security Plan
- 4.4 Incident Response
- 4.5 Metrics
- 4.6 Personnel Information Security

5. Operational Security Plans

- 5.1 'Absolutely Necessary' Security Standards
- 5.2 'Highly Recommended' Security Practices.

6. Audit Standards

Security is a Partnership

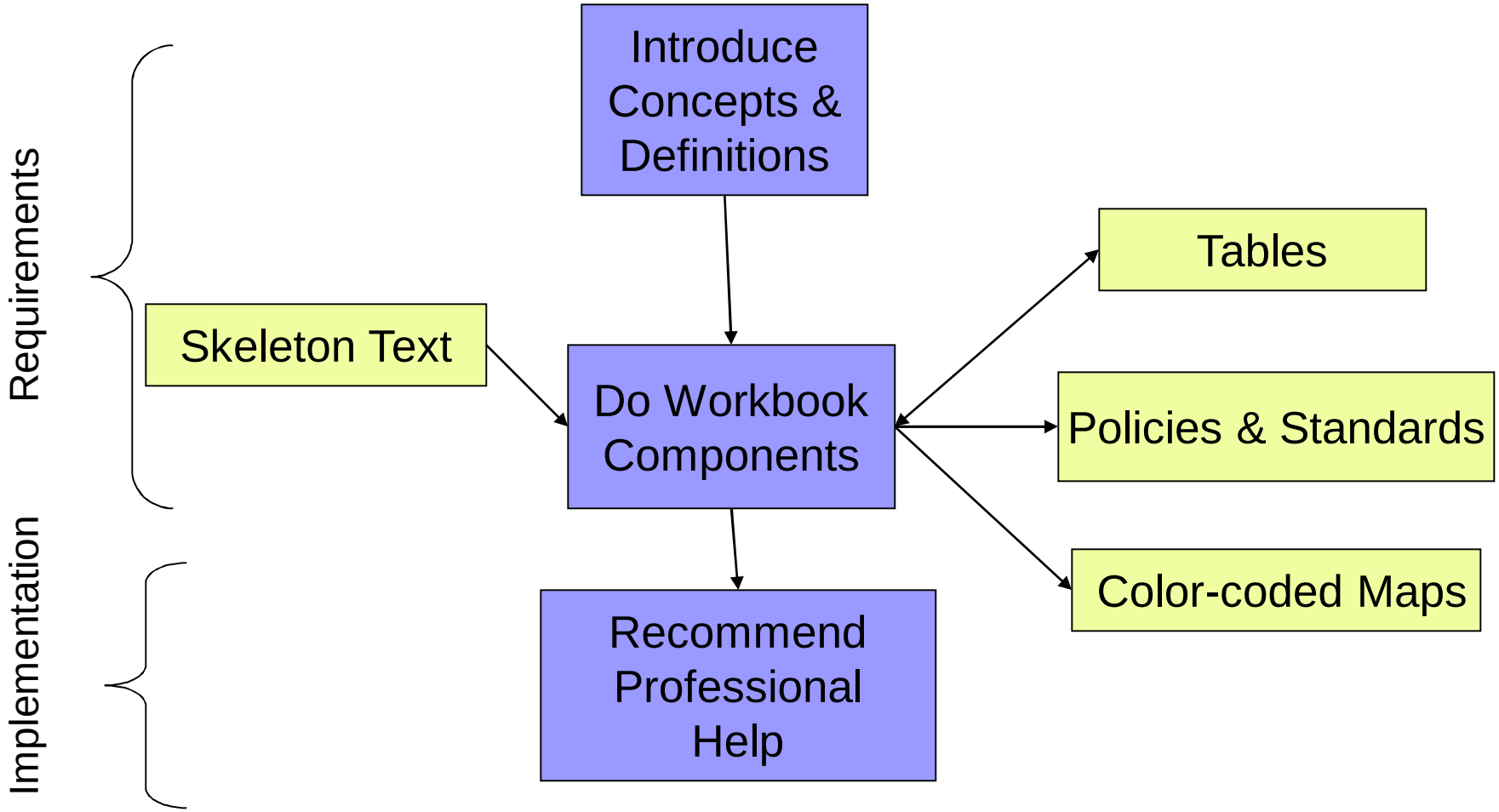
Business

- What to protect
- How much it will cost

Technology

- How best to protect
- How to detect and recover

Purpose of Workbook: Define Security Requirements


Requirements
Implementation
Introduce Concepts & Definitions
Skeleton Text
Do Workbook Components
Recommend Professional Help
Tables
Policies & Standards
Color-coded Maps

Code of Ethics Skeleton

This code of ethics provides general guidelines, and is not intended to cover every potential scenario. Examples are provided only as necessary for the employee to understand general concepts.

General Employee Conduct While at Work

Employees are expected to work overtime when patients remain in the office after hours, until the doctor on staff gives permission to leave.

HIPAA guidelines are to be followed, on potential penalty of firing, fines, and jail time.

Unethical Behavior

Conflict of Interest

Confidentiality

Relationship with Customers and Suppliers

Gifts & Entertainment

Using the Organization's Assets for Personal Activities

Reporting Fraud or Unethical Behavior

[1] This Code of Ethics is adapted from "Essentials of Corporate Fraud", Tracy L Coenen, John Wiley & Sons, 2008.

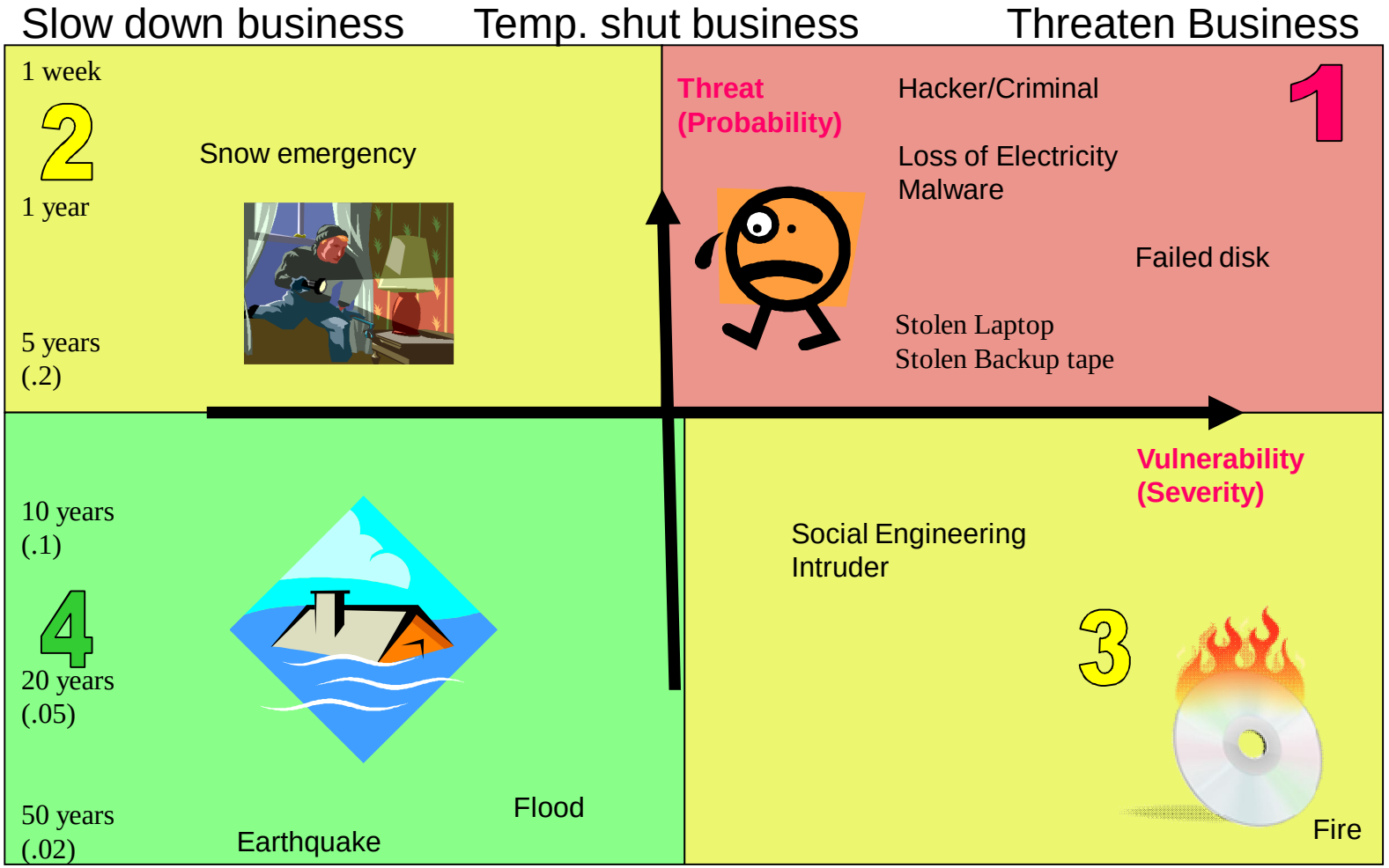
Skeleton Policy - Example

Access Control

Least privilege ensures that computer access is provided only on an as-needed basis, and is a mandatory aspect of HIPAA for employees and business associates alike. All computer access requires individual authentication, and access to software, hardware, and data is controlled. Data owners decide access to data views, and this access is reviewed at least annually.

Qualitative Risk

Vulnerability Assessment Quadrant Map



Quantitative Risk

Step 1: Assign Assets to Assets

Asset	Direct Loss	Consequential Loss	CIA & Notes
Office Building	250,000	Daily Op (DO)	Avail.
Medical Database	10,000	DO + Mal + Hip + Brch	CIA
Laptop	2,000	DO + Mal + Hip	Conf/Avail

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence	Annual Loss Expectancy
Facility	Fire	$200,K	0.01	$2,000
Medical Office	Malpractice	$1M	0.05	$50,000
Medical Info	Stolen (Copied) (Hacker,malware, fraud)	$150,000 = $50K Liability + $100K Salary + notification	1.0	$150,000

Step 2: Determine Loss due to Threats & Vulnerabilities

Step 3: Estimate Likelihood of Exploitation

Risk Table: Treat Risk

Risk	ALE Score	Control	Cost of Control
Malpractice	$50,000	Medical server up	
Social Engineering	$25,000	Awareness training HIPAA Adherence	Weekly HIPAA meetings, Annual training
Stolen Information/ HIPAA audit	$15,000	HIPAA Adherence, Encrypted disks, VPN, firewalls, antivirus software, Audit tech/service	Weekly HIPAA meetings, Encryption & security technology
Bad server disk			
Stolen laptop			
Power Failure			
Fire			
Failed Comm			

Step 4: Compute Expected Loss

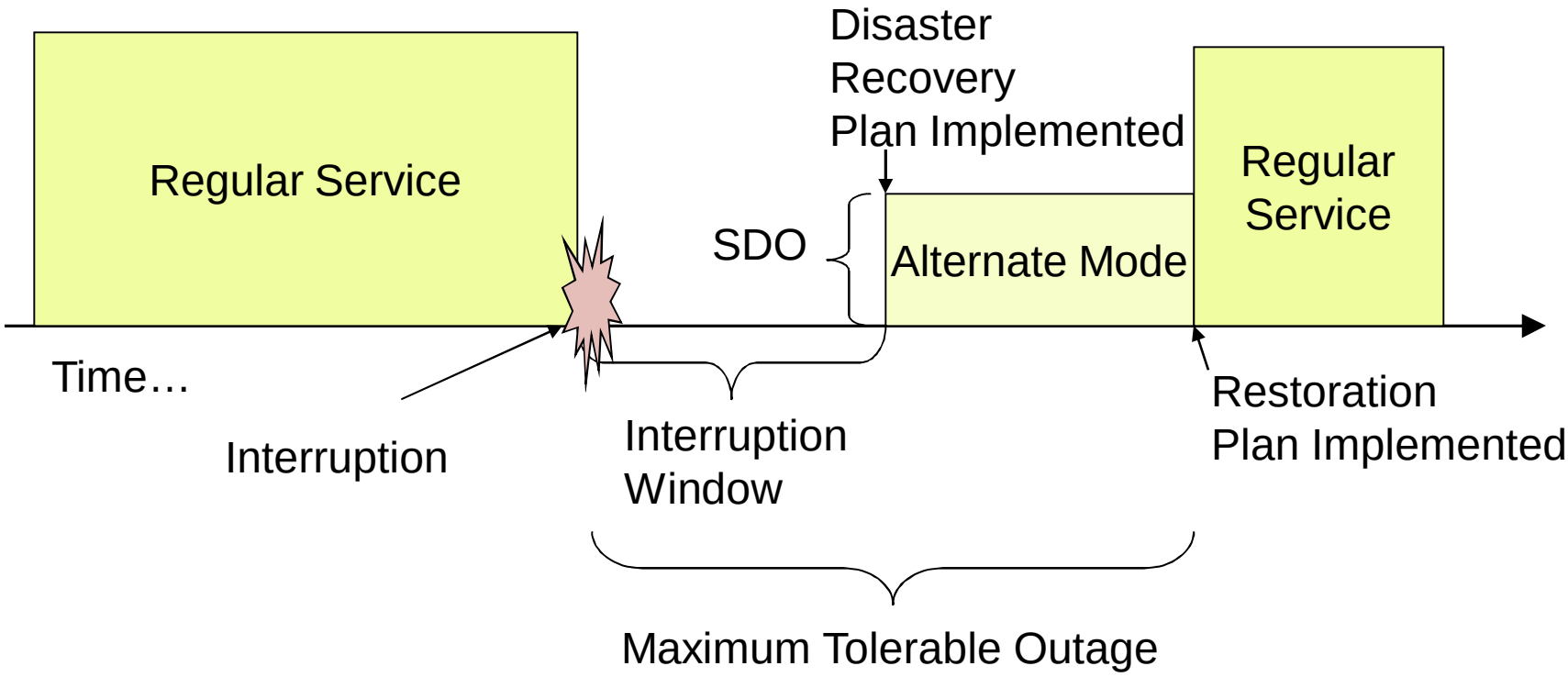
Step 5: Treat Risk

Introduce Concepts: Recovery Terms

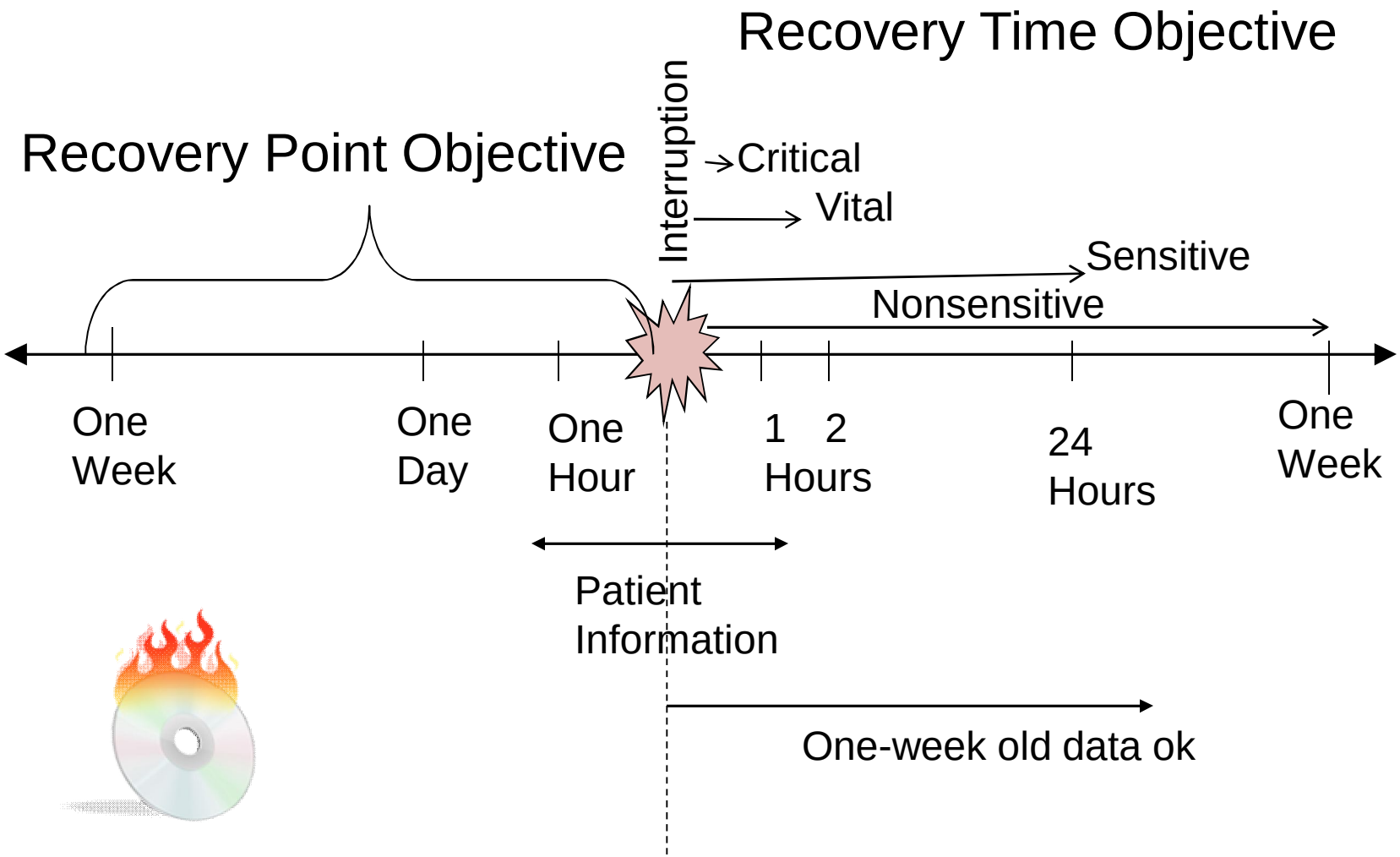
Interruption Window: Time duration organization can wait between point of failure and service resumption

Service Delivery Objective (SDO): Level of service in Alternate Mode

Maximum Tolerable Outage: Max time in Alternate Mode



Introduce Terms: RPO & RTO



BIA & Business Continuity

Step 1: Define RPO, RTO

Service	RPO (Hours)	RTO (Hours)	Critical Resources	Special Notes
Patient Service	1 hour	0-2 hours	Computer system	Can operate with Patient DB being up to one week old for 2-3 days.

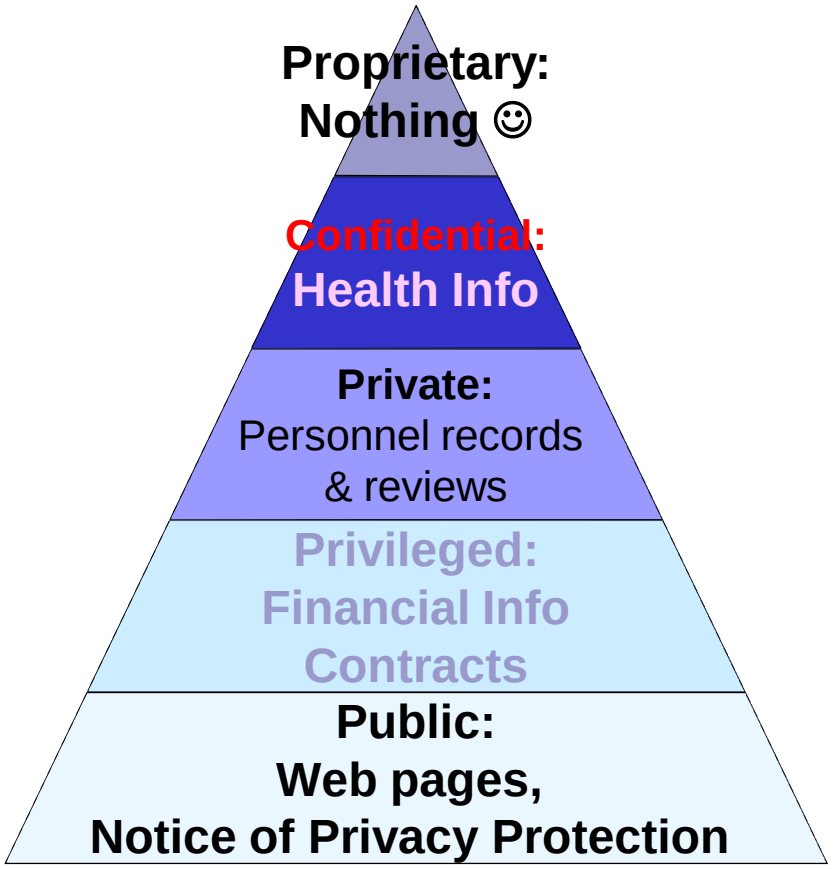
Step 2: Define Control Technologies

Data File and System/Directory Location	RPO (Hours)	Special Treatment (Backup period, RAID, File Retention Strategies)
Patient Service	none, 1day	RAID, Offsite backup/restore

Step 3: Define Problem Events & Procedures (Backup/Restore…)

Sensitivity Classification

(Example)



Classify Data by Sensitivity

Sensitivity Class	Description	Information Covered
Confidential	Information **protected by HIPAA or other law.** Shall be made available or visible on a **need-to-know** basis only. Dissemination could result in financial liability or reputation loss.	Health care information: PHI & EPHI Personnel records & reviews
Privileged	Accessible to management or affected parties only. Could cause **internal strife or external embarrassment** if released.	Financial Database Budget Third party contracts

Define Treatment by Sensitivity Class

	Confidential	Privileged
Access	Need to know	Need to know
Paper Storage	Locked cabinet, Locked room if unattended	Locked cabinet Locked room if unattended
Disk Storage	Server-only storage Password-protected, Encrypted, Hashed	Password-Protected
Labeling & Handling	'Confidential' Clean desk, low voice, shut doors	Clean desk
Transmission	Encrypted	Local only, Encr.
Archive	Encrypted	
Disposal	Degauss & damage disks Shred paper	Reformat disks

Define Asset Inventory

Asset Name	Patient Information
Value to Org.	Crucial to patient health, affects liability
Location	Secure Data Room
Criticality & Sensitivity Class	Confidential, Vital
IS System	Patient Database
Data Owner	Jamie
Designated Custodian	Backup Ops: Terry IS Operations: Pat C.

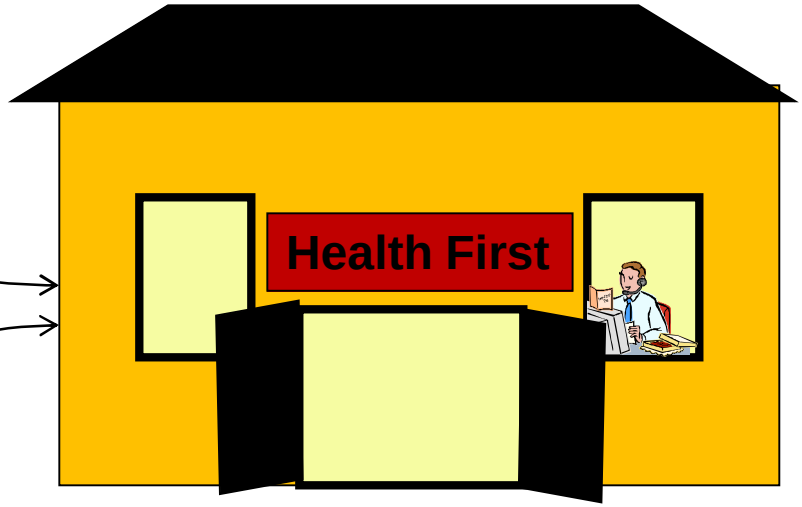
Role-Based Access Control

Role Name	Information Access and Permissions (e.g. RWX)
Admin	RW Access: 6.1 Patient Appointment 6.2 Patient Information 6.3 Patient Medical History 6.5 Patient Plan Management 6.6 Health Plan Eligibility 6.8 Health Care Claim Status 6.10 Health Care Payment
R.D.	RW Access: 6.4 Patient Medical Treatment (R for Prescription) 6.7 Health Care Claim
M.D.	RW Access 6.4 Patient Medical Treatment 6.7 Health Care Claim 6.9 Certification and Authorization of Referrals

Network Security: From where is data accessed?

HMO/PPO: Billing
Authorizations, Referrals

Hospital
Chris: Patient Care
Personnel (Local)



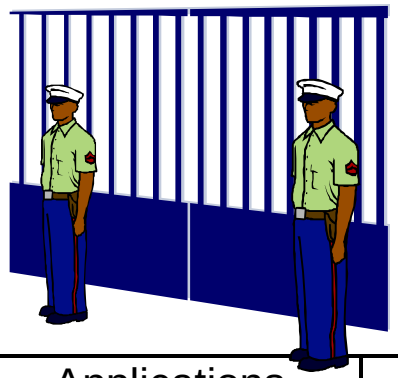
Patient
Care

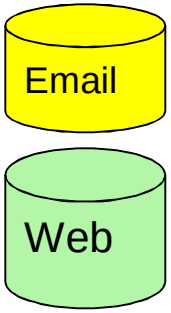
At home – Jamie: Patient Care, Finances (local)

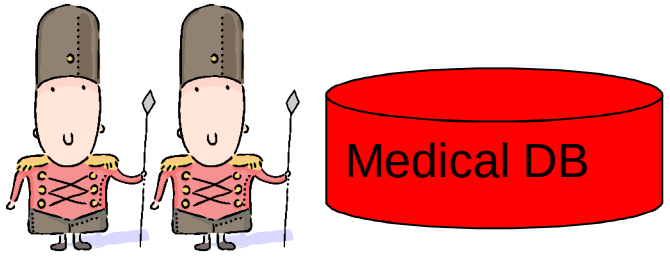
Terry At Health First:
Patient Scheduling
Patient History

Networked Applications

Service	Sensitivity	Roles	Server
Medical Database	Confidential	Staff	Medical
Finance	Private	Partner	Operations

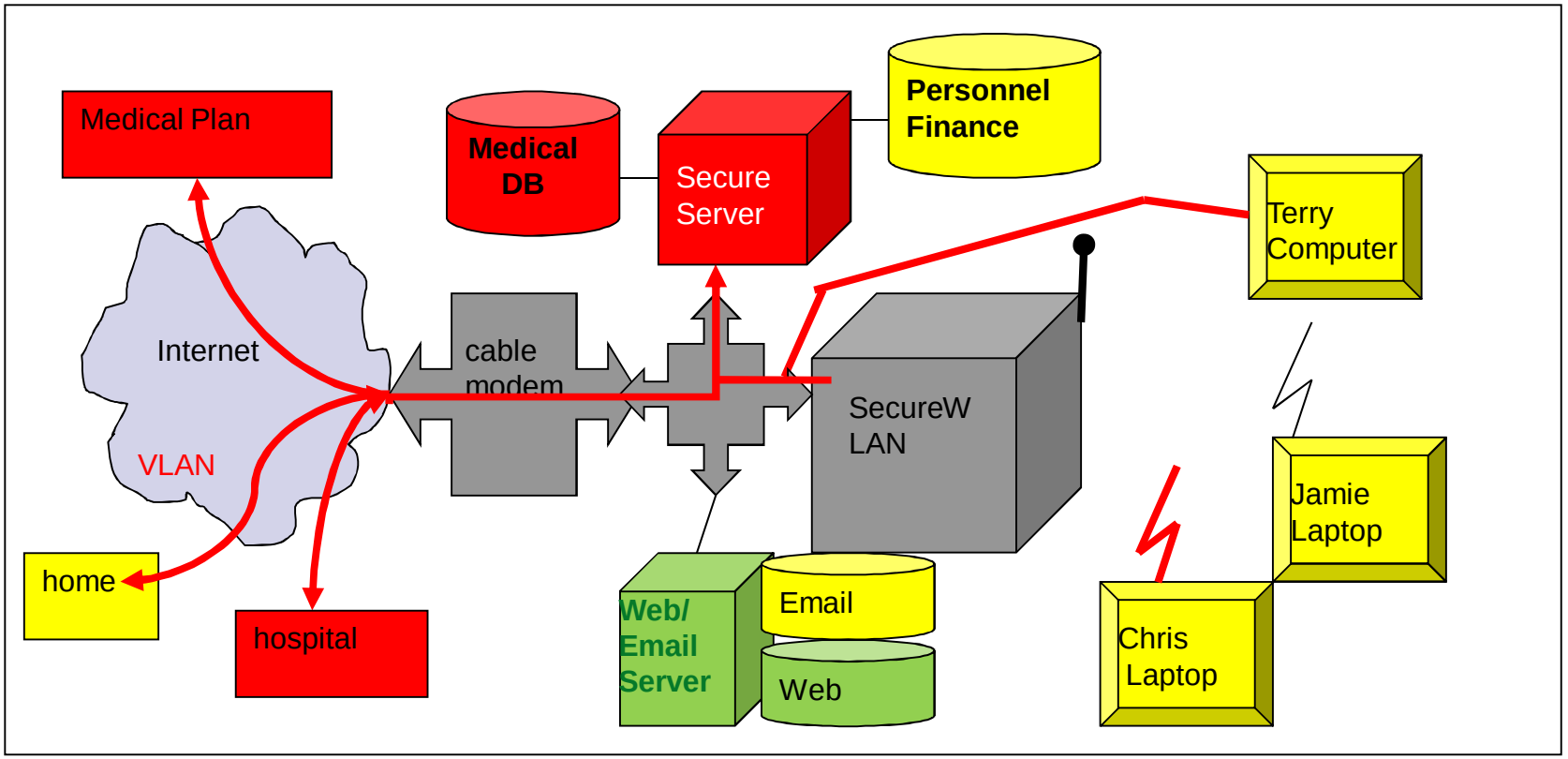




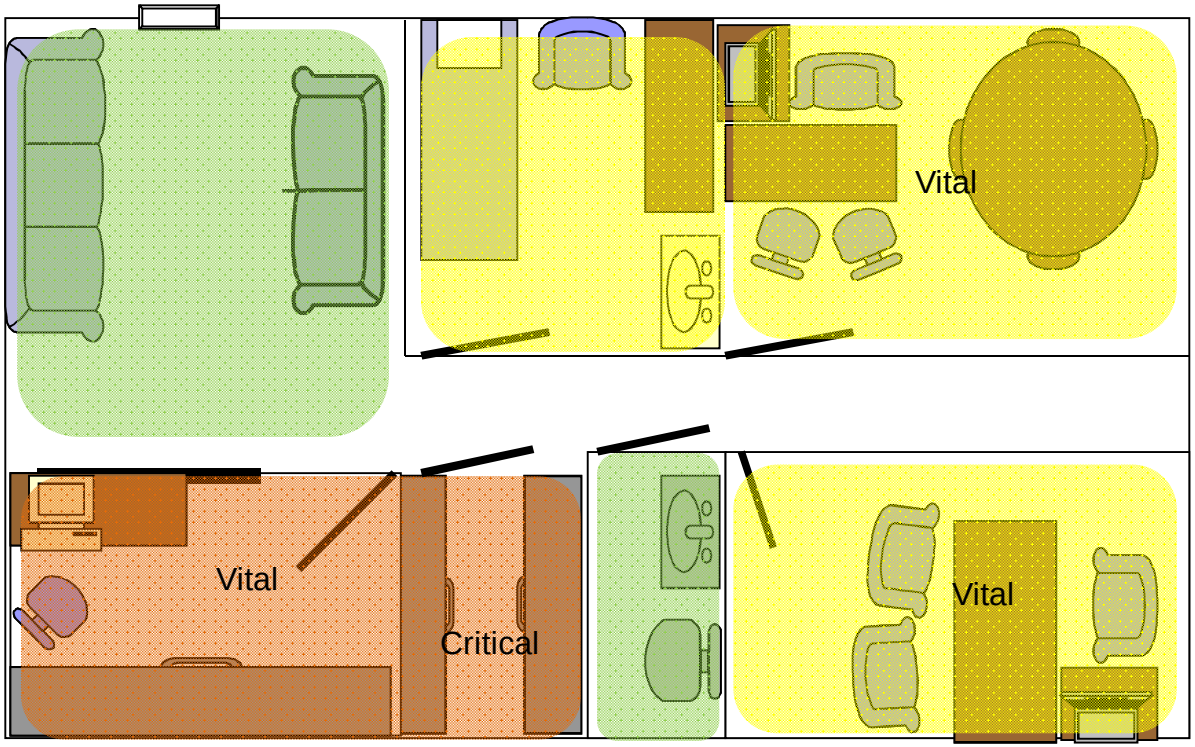


Applications	Sources of Entry	Servers	Required Controls (e.g., Encryption)
Medical Database	Office, Home, Hospital	Medical Database Server <only>	Encryption VPN
Medical Transactions	HMOs/PPOs	Medical Database Server	Encryption, specialized protocols

Network Security Map with Color-Coding



Physical Security Map with Color-Coding



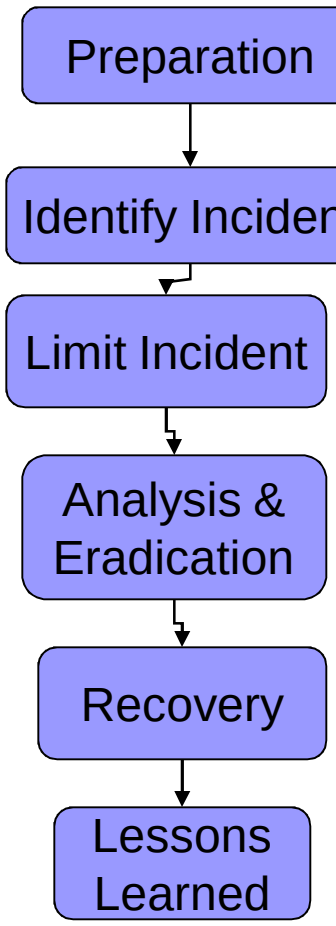
Sensitivity Classification:

- Green= Public
- Yellow= Sensitive
  - Confidential Access
- Orange=Private
- Red=Confidential
  - Confidential Data Storage
  - No patients
  - Cabinets locked
  - Room locked

Criticality Classification:

- Critical: Air conditioning, UPS, fire suppressant, etc.

Incident Response Plan



Determine and remove root cause

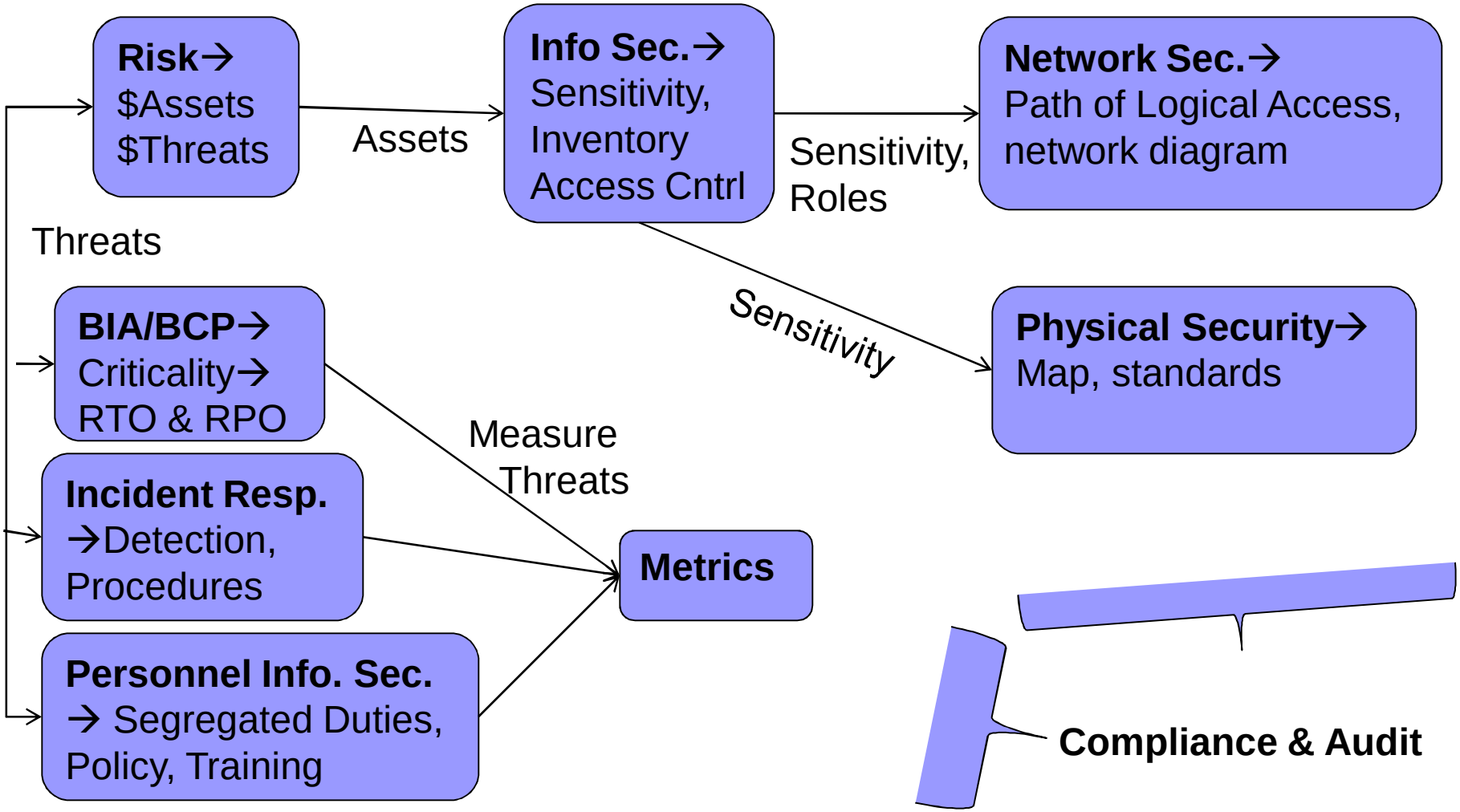
Return operations to normal

Process improvement: Plan for the future

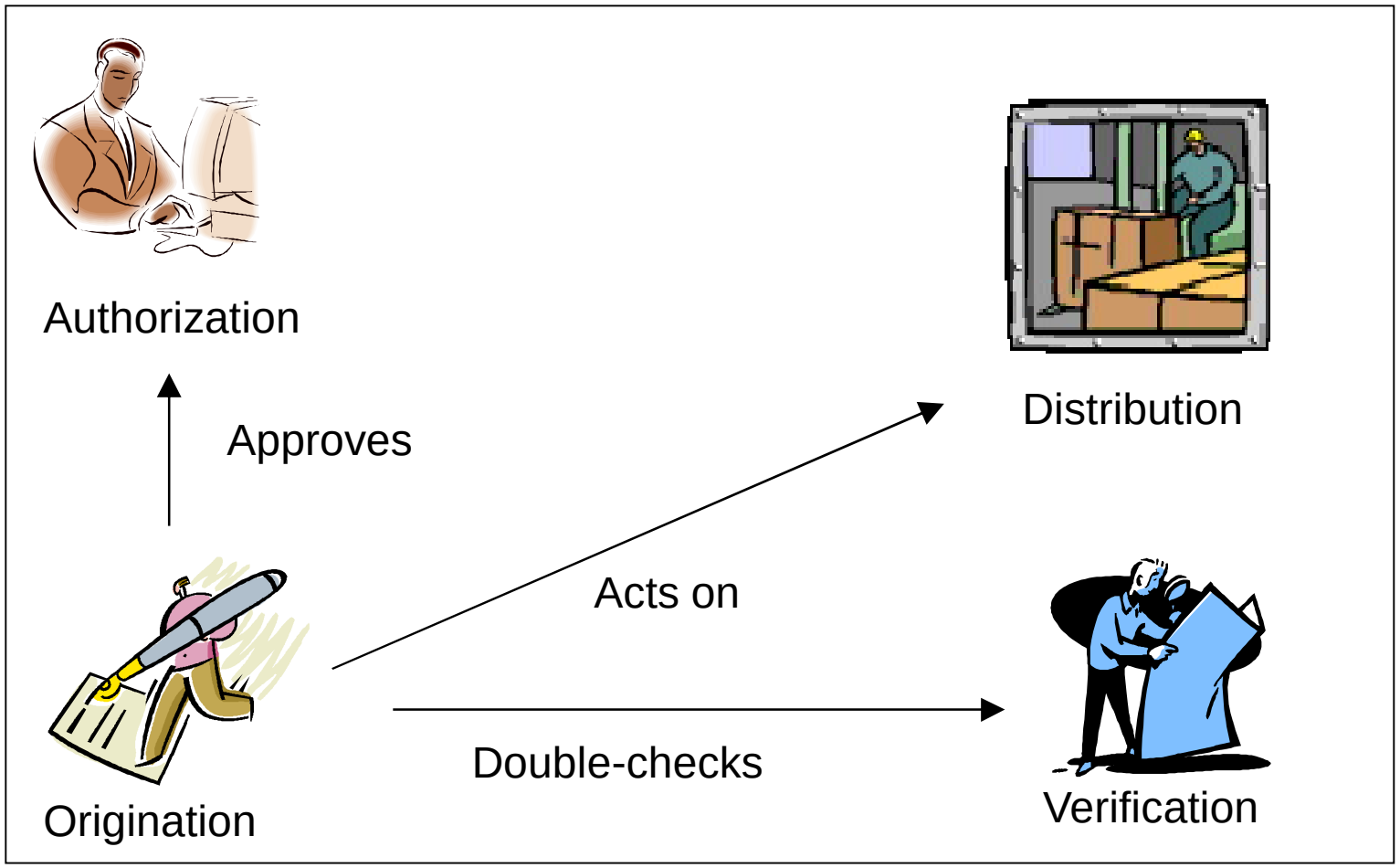
Incident	Description	Methods of Detection	Procedural Response
Hacker Intrusion	An intruder has entered the local network.	Last login; Weekly log checks; Antivirus Email alarm	Table 4.4.2 Hacker Intrusion Incident Response

Incident Type: Hacker intrusion
Contact Name & Info:
Emergency Triage Proc:
Escalation Conditions and Steps:
Analysis & Eradication Proc:
Other Notes (Prevention techniques): .

Top-Down Information Security → Security System



Personnel Security: Define Segregation of Duties



Who could subvert the system?

Fraud Problem

False new patient

Unreported cash patients

Selling drugs

Selling health info

Legal Implication

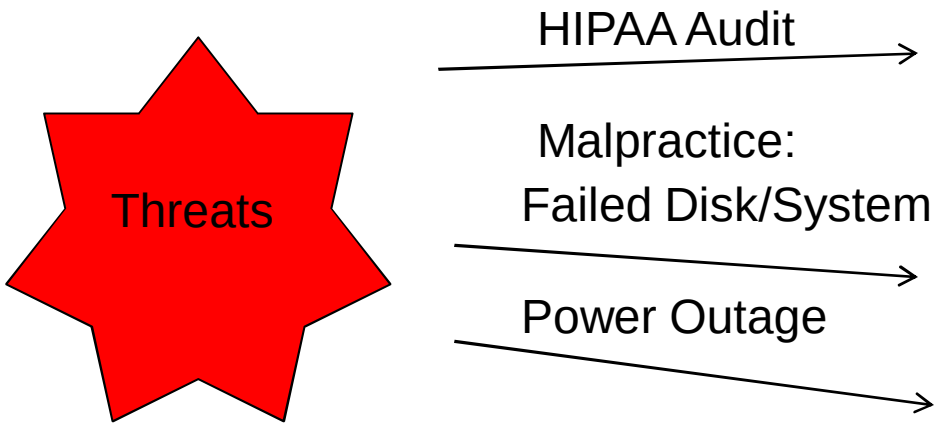
- **Medicare/HMO fraud**
- **Theft or tax evasion**
- **Malpractice**
- **HIPAA, Notification Act violation**

Threat	Role	Control
False new patient	**Admin**	**Weekly audit meeting to review: Medical DB Access Report**
Unreported cash patients	**Admin**	**Weekly audit meeting to review: Medical DB Access Report**

Allocate responsibility for security

Chief Security Officer: **Terry** 	Person responsible for security project management **Take backup tapes daily** **Lead weekly audit meeting, providing Medical DB Access Report** **Perform physical inventory weekly (except partners' laptops)** **Collect security metrics** **Provide HIPAA and procedural security training** **Complete Incident Response Report when necessary**

Developing Metrics



Annual Audit
Weekly visits by KSC
Attendance at audit meetings

Hours without DB service
Time to detect & contain incidents

Category	Metric	Calculation & Collection Method	Period Reporting
Strategic	HIPAA Audit Performance	Health First Team	Annual
	Computer Security Audit	Kenosha Software Audit Plan	Twice yearly
Tactical	Hours without DB service	Patient DB Outage Form	Twice yearly
	Attendance at Audit meetings	Monthly audit meetings	Twice yearly

Conclusion
Goals are to…

Help small businesses

- Plan for security
  - Achieve near-COBIT Level 3
- Security Awareness Training
- Audit

Train Students

- Provide lectures on security
- Train students for CISA & CISM certification
- Help students gain valuable experience

Security Workbook Features

- Just-in-time security concepts
- Skeleton versions of text/tables
- Visual aids (color-coded maps)
- Build system of security
- Phased approach
- Security & teaching aids

Download of Workbook & Materials Available

If you would like to use the Security Workbook, Lectures, or Case Study

Indicate so on the form…

lincke@uwp.edu