E-Record Privacy

ARMA Chicago Workshop
September 13, 2005

Daryl L. Thompson
Thompson Network Consulting

E-Record Privacy

- E-Record Privacy
  - Definition
  - Motivations
  - Threats
- Achieving E-Record Privacy
  - Security Definition
  - Security Model Evolution
  - Security Process
- References

What Record Privacy Is Not

- This year, the University of Chicago Hospitals reported that a former employee had stolen information on as many as 85 patients.
- In Florida, an employee at the Palm Beach County Health Department mistakenly emailed the names of AIDS patients.
- Administrators at UC Berkeley acknowledged that a computer laptop containing the names and Social Security numbers of nearly 100,000 people - mostly graduate school applicants - had been stolen

E-Record Access Process

- E-Record Users are:
  - Employees
  - Third Party Partners
  - Customers/Clients/Patients
  - Computer Systems (Web Services)
- E-Records can be Accessed Through:
  - Company Intranet
  - Internet
- E-Record User Identification Credentials
  - Something You Know: Usernames/Passwords
  - Something You Are: Fingerprint/Eye Scan
  - Something You Have: Token
  - Something You Trust: Certificate Authority

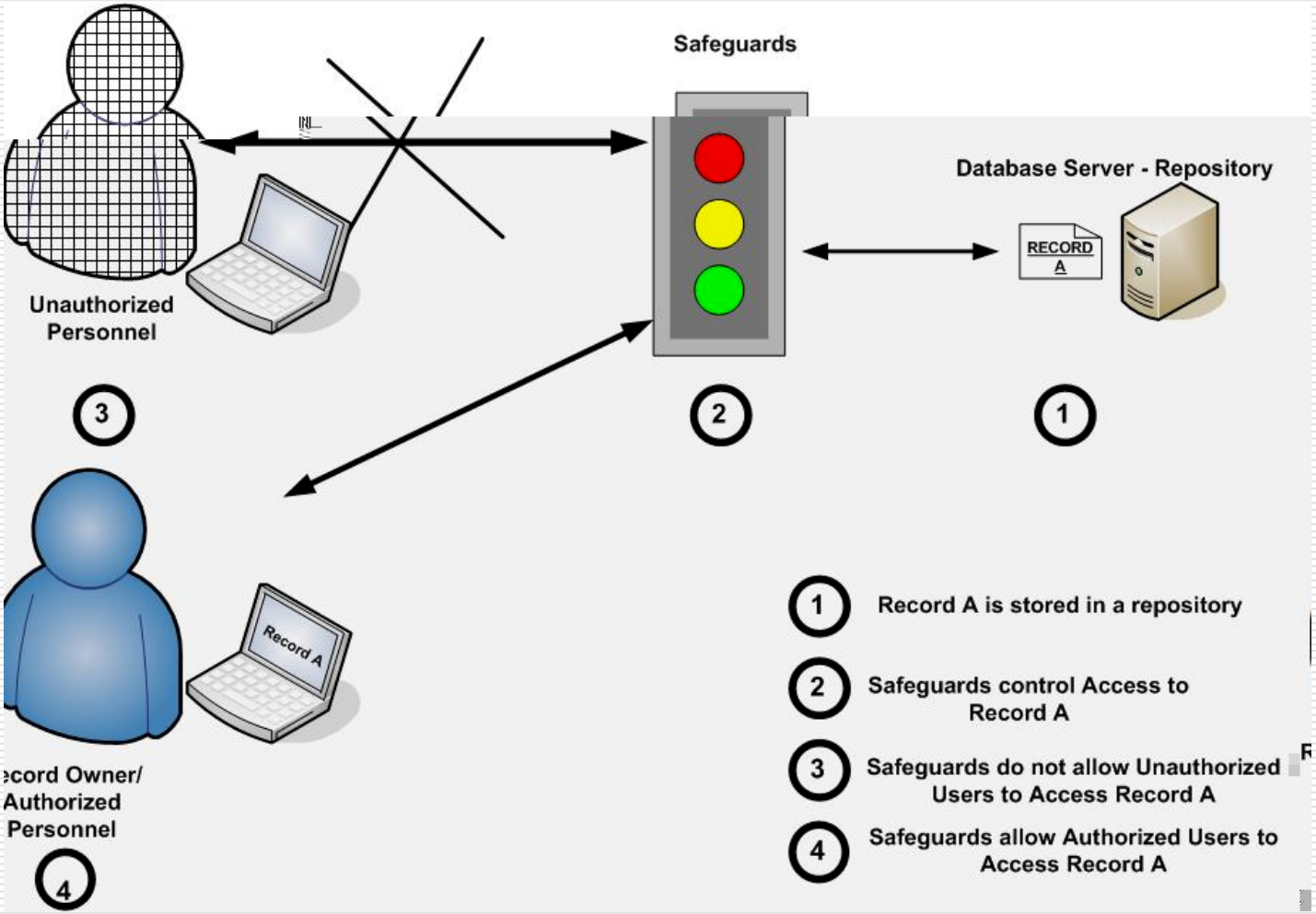
E-Record Access Process

- Users present credentials to access E-Records
- Users perform actions on an E-Record.
- The access medium can be the company network, or the Internet.

E-Record Privacy - Definition

- Access to E-Records should be restricted to Authorized Users
  - Record Management determines Authorized E-Record Users
  - Controls and Safeguards restrict Unauthorized Users
- E-Record Privacy defines Trust Relationships, whereby:
  - User access is Confidential
  - Users perform authorized E-Record actions
  - User actions are tracked
  - E-Record integrity is maintained
  - Users assured of E-Record Authenticity

E-Record Privacy -Example



E-Record Privacy Safeguards

- Controls utilized to restrict unauthorized E-Record access
  - Administrative
    - Policies, Standards, Procedures
    - Personnel Screening
    - Employee Training
  - Technical
    - Access Controls (passwords, biometrics, …)
    - Encryption
    - Security Devices (Firewalls, Intrusion Detection)
    - Electronic Document Security
  - Physical
    - Facility Protection
    - Security Guards
    - Locks, Monitoring

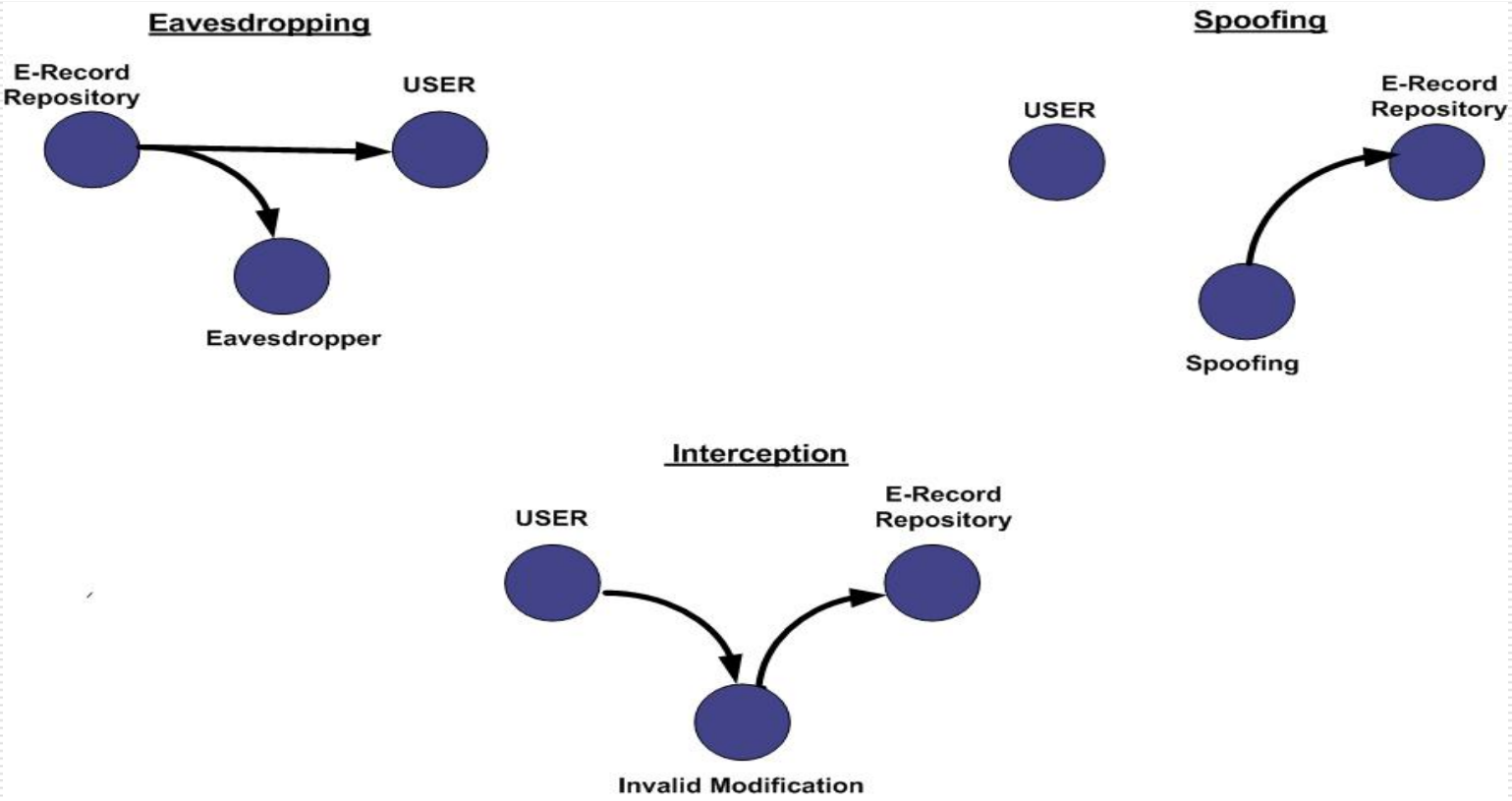
Why do Organizations need E-Record Privacy?

- Prevent unintentional E-record disclosures
  - Confidential Business Information
  - Private Customer Data
- Compliance with regulations
  - 21 CFR 11, HIPAA, Sarbanes-Oxley
- Good Business Practices
  - Ensure E-Record integrity and consistency
  - Detect malicious behavior

E-Record Privacy – Threat Examples

- Malicious E-Record Monitoring/Modification
  - Eavesdropping
    - Reading/Monitoring E-Records during transmission
  - Interception
    - Capturing E-Records during transmission and modifying E-Record content
  - Spoofing
    - Impersonating an E-Record User with Access Rights
    - Exploiting weak E-Record Safeguards to Access an E-Record
  - Most Record Privacy violations are “Inside Jobs”

E-Record Privacy - Threat Examples



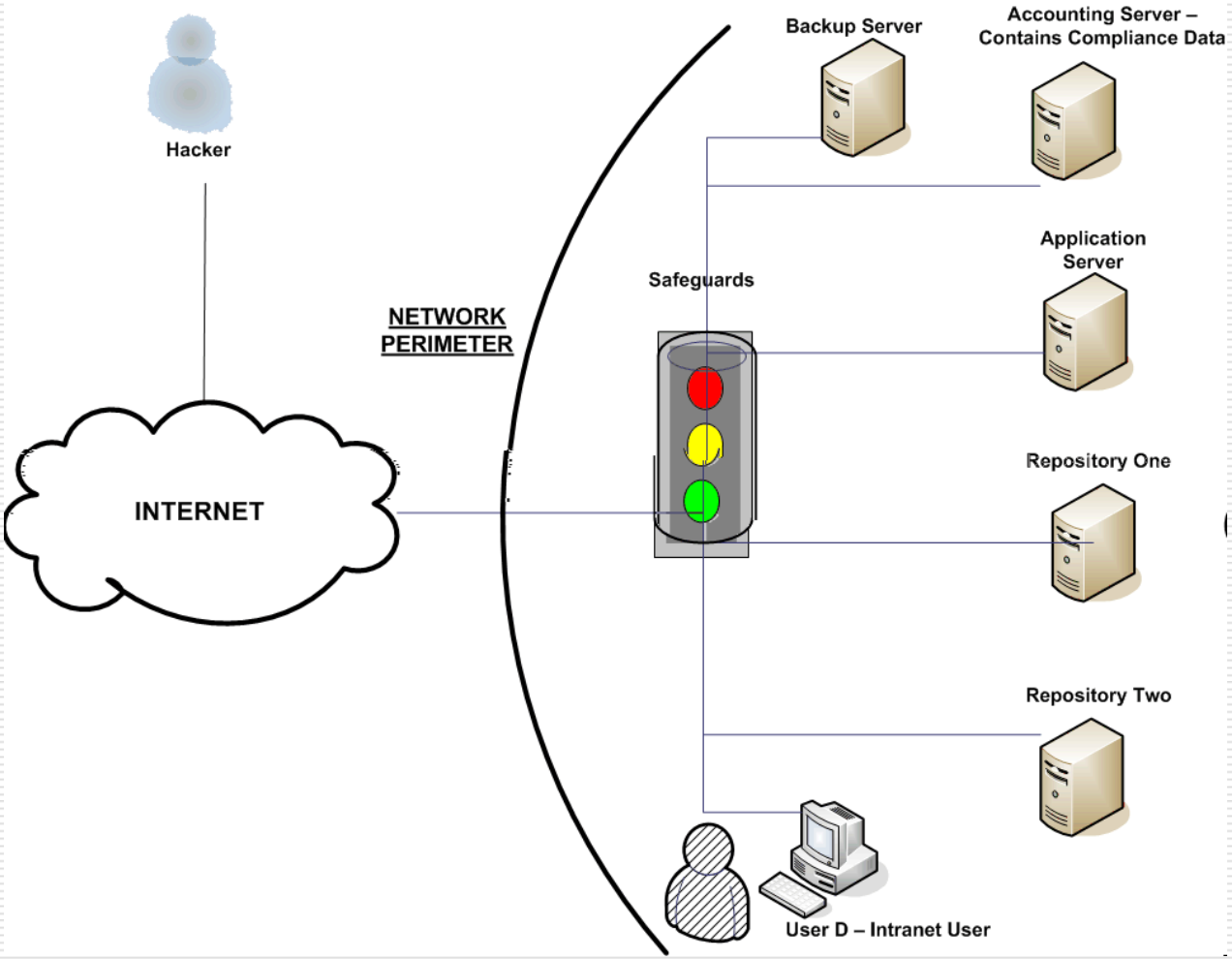
Achieving E-Record Privacy –Security Definition

- Information Systems Security processes enable E-Record Privacy
  - Security Safeguards protect Organizational Assets
    - Hardware
    - Software
    - E-Records
  - Security is Evolving
    - Past: Protect Computer Network Perimeter
    - Now: Verifying E-Record Users, E-Record Security

Information Systems Security – Evolution

- Historically, Information Security was concerned with protecting the Network Perimeter
  - Clear knowledge of:
    - E-Record User locations
    - Network Outside/Network Inside defined
  - Safeguards addressing Network Threats
    - Installing Firewalls
    - Detection Systems for identifying viruses
  - Network Perimeter protection and Information Security solutions primarily an IT department responsibility
  - Trust Relationships are well defined

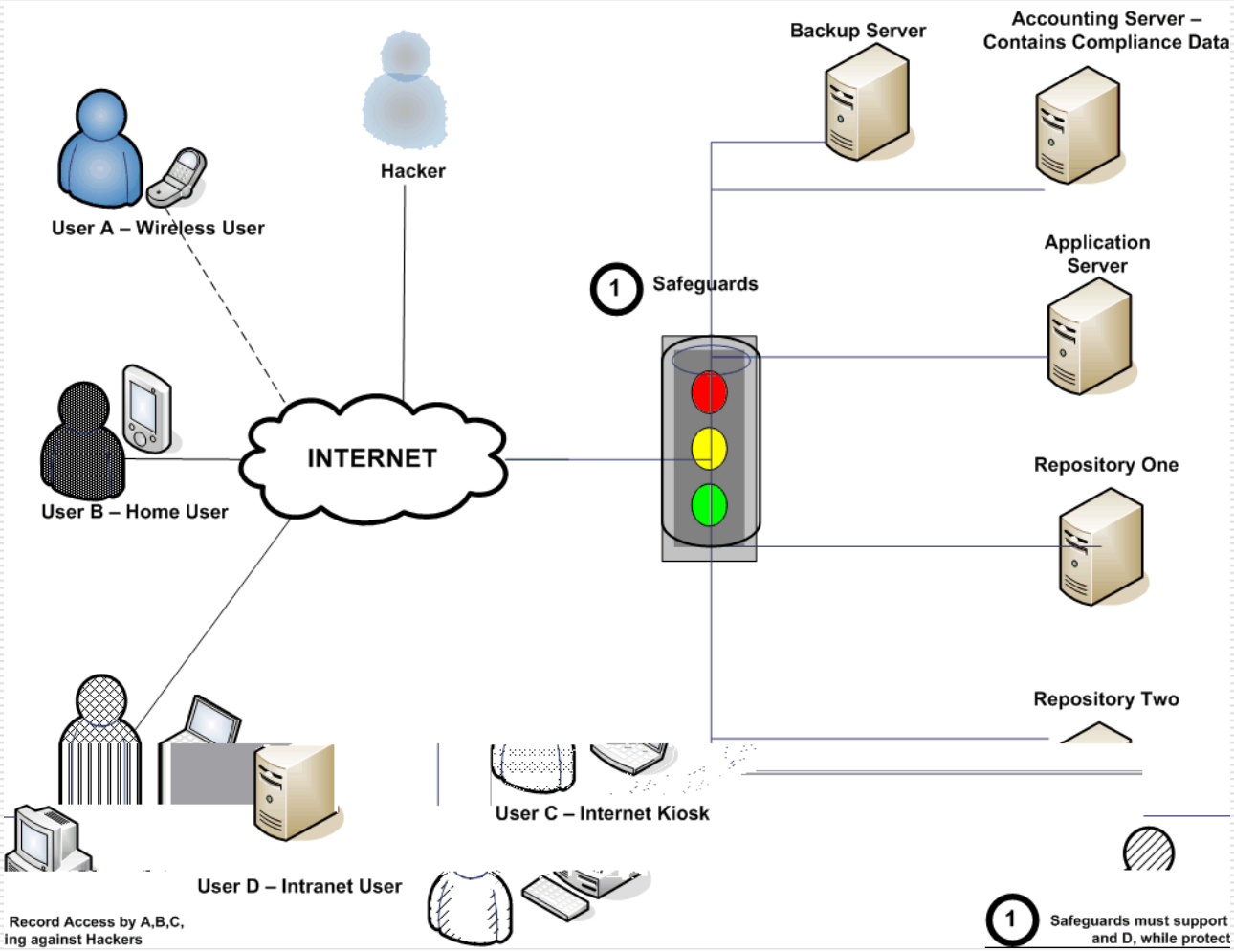
Past Security Perspective



Achieving E-Record Privacy – Now

- Network Perimeter is gone
  - E-Record Access is accomplished from a variety of locations
    - Remotely from Home/Internet Kiosks
    - Wireless connections
  - Organization work relationships change
    - 3rd party partnerships/Outsourcing
  - Trust Relationships must account for:
    - E-Record Lifecycle
    - Business Process Workflow
    - Employee Type and Lifecycle
- Support Trust Relationships while preventing:
  - Eavesdropping
  - Interception
  - Spoofing

Record Privacy – No Network Boundaries



Achieving Record Privacy – Challenges

- User Location
  - Should remote Users have the same E-Record access permissions when using their home PC?
- E-Record Lifecycle
  - E-Record access rights change throughout the lifecycle
- Employee Lifecycle
  - E-Record access rights should be updated with personnel changes
- General
  - Preventing unauthorized E-Record disclosures
- Safeguards must adjust to maintain E-Record privacy

Achieving Record Privacy – E-Records

- Acivacy – g Record is a collaboration:-Records

Information Security - Process Steps

- Risk Analysis
  - Identify Privacy Risks
  - Rank risks in order of potential damage to organization
  - Identify reasonable Safeguards to address risk
- Secure
  - Implement Safeguards
- Monitor/Test
  - Monitor Safeguard Effectiveness in providing E-Record Security
  - Test E-Record Privacy implementation
- Manage/Improve
  - Based on Monitor/Test data, Identify improvement needs
- Security is an iterative process
- There is never a 100% solution, always Risk to address.

E-Record Privacy

- Reasonable Security safeguards must reduce the frequency and severity of security related losses
  - Due diligence
    - Proper investigation of Computer System weaknesses
  - Due Care
    - Reasonable actions to prevent security breaches
      - Anti-Virus Controls
      - Employee Education
      - Firewalls
      - Locks
    - Limiting damages when security breaches occur
- Costs should not exceed benefits
- A sound security program is smart business practice

Information Security - Requirements

- Successful E-Record Privacy programs have:
  - Total Organizational Commitment to Security
  - Employee Training
  - IT Systems Accounting and Auditing
  - Business Continuity/Disaster Recovery planning to ensure E-Record Availability

References

Information Nation: Seven Keys to Information Management Compliance - Randolph A. Kahn Esq. and Barclay T. Blair

The Practical Guide to HIPAA Privacy and Security Compliance - Kevin Beaver and Rebecca Herold

Stay Safe Online - www.staysafeonline.info

Information Technology Governance - http://www.itgovernance.com

Description of common Information Technology terms and acronyms - http://www.webopedia.com

Thank You

ARMA Chicago-Chapter President: Doris Hambacher

Education Committee Co-Chair: Susan Izban

Education Committee Co-Chair: Dernea Michaux-Davis

Questions???

Daryl L. Thompson
darylthompson@thompsnet.com
www.thompsnet.com
708-214-7544