Regulatory Compliance & Information Security

Uday Ali Pabrai, CISSP, CSCS
Author, Get Compliant. Get Secure!

Healthcare Industry Challenges

- Largest industry in the USA
  - 17% of the U.S. gross domestic product
  - Growing faster than the economy
- Significant challenges
  - Medical errors – 8th leading cause of death (HBR May 2006)
  - 250,000 people die in the U.S. each year due to surgical errors, mistaken diagnostics, incorrect prescribing, hospital-acquired infections and inadequate care (IBM July 2006)
  - 46 million uninsured in the U.S.
- Future is about innovation and integration of technology
  - Increase efficiency, improve care, and save consumers time

ecfirst.com HEALTHCARE

Technology Challenges

- **Too many servers**
- **Too many applications**
- **Too many PCs to maintain and manage**
- **Mobility of devices is rapidly increasing**
- **Storage demands are increasing fast**
- **Highly specialized technical skills required**
- **Serious lack of redundancy**

ecfirst.com
HEALTHCARE

National Health Information Network (NHIN)

- NHIN Definition:
  - A “network of networks”
  - Built on the Internet
  - Making all patient Electronic Health Record (EHR) available nationwide, online, real-time, wherever healthcare is provided
- Information on NHIN must be secure and exchanged in a patient-centric manner and governed by privacy and access control policies
- State of the art and stringent security features are a critical component of NHIN if privacy is going to be preserved

ecfirst.com HEALTHCARE

Compliance Challenges

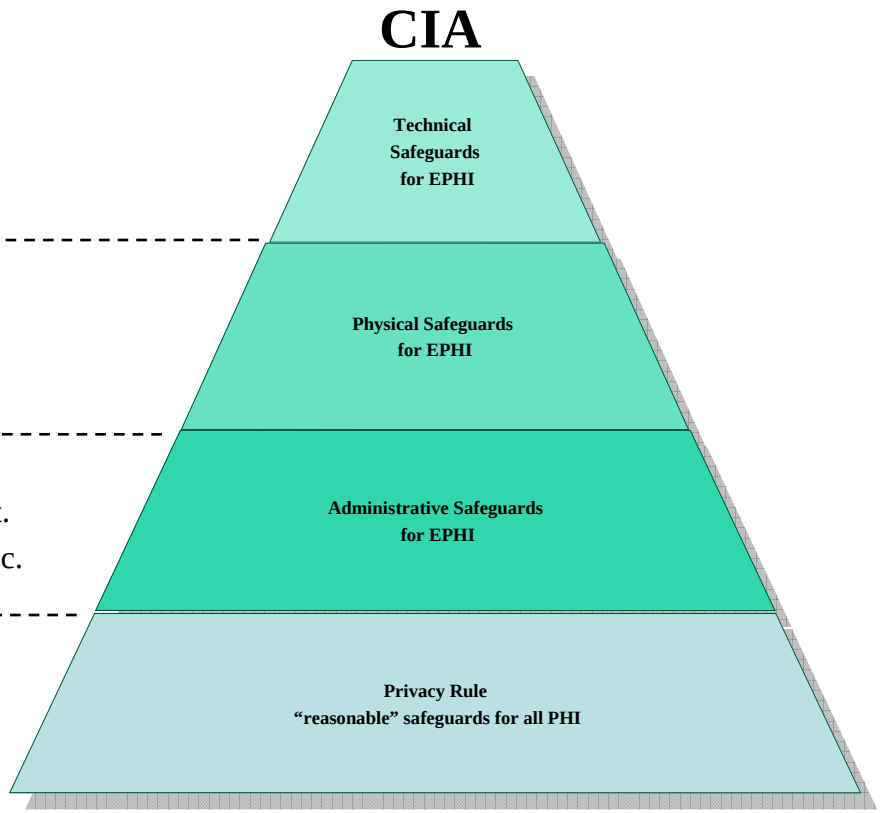
ecfirst.com
HEALTHCARE

Healthcare

- Access Control
- Audit Control
- Integrity
- Person or Entity Authentication
- Transmission Security

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

- Security Mgmt. Process, Sec. Officer
- Workforce Security, Info. Access Mgmt.
- Security Training, Security Incident Proc.
- Contingency Plan, Evaluation, BACs



ecfirst.com
HEALTHCARE

Financial

- Sarbanes-Oxley Act of 2002 is having an impact on an organization's IT, especially security systems, practices and controls
- Section 404 is a critical part of legislation
  - Requires an internal control report
- Areas of security that require particular attention include:
  - Secure identity management
  - Data integrity
  - Automated audit capabilities

ecfirst.com
HEALTHCARE

U.S. Government

- The Federal Information Security Management Act (FISMA) is Title III of the U.S. E-Government Act (Public Law 107-347)
- It was signed into law by U.S. President George W. Bush in December 2002.
- FISMA impacts all U.S. federal information systems
- The FISMA legislation is about protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide CIA

ecfirst.com
HEALTHCARE

State Legislations

- The California Information Practice Act or Senate Bill 1386 (SB 1386) requires organizations conducting business in California to disclose any security breach that occurs to any California resident whose unencrypted personal information was, or is, reasonably believed to have been acquired by an unauthorized person
- The California Assembly Bill 1950 (AB 1950) expands on the privacy requirements of SB 1386 and requires that organizations take “reasonable precautions” to protect California residents’ personal data from modification, deletion, disclosure, and misuse rather than just report on its disclosure

ecfirst.com
HEALTHCARE

International

ISO 17799: 2005 Covers These Areas:

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

ecfirst.com
HEALTHCARE

Security Challenges

ecfirst.com
HEALTHCARE

Under Siege, Rising Threat

- Large, multipurpose attacks on network perimeters
- Rising threat includes focused attacks on client-side targets
- Targeted attacks on Web applications and Web browsers are the focal point for cybercriminals
- Threats are now motivated by profit
- Financial services is the most frequently attacked industry

How confident are you about your organization's information security posture?

ecfirst.com
HEALTHCARE

Security Challenges

- “99% of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures are available”

NIST

- **Increased dependence on electronic information and infrastructure**

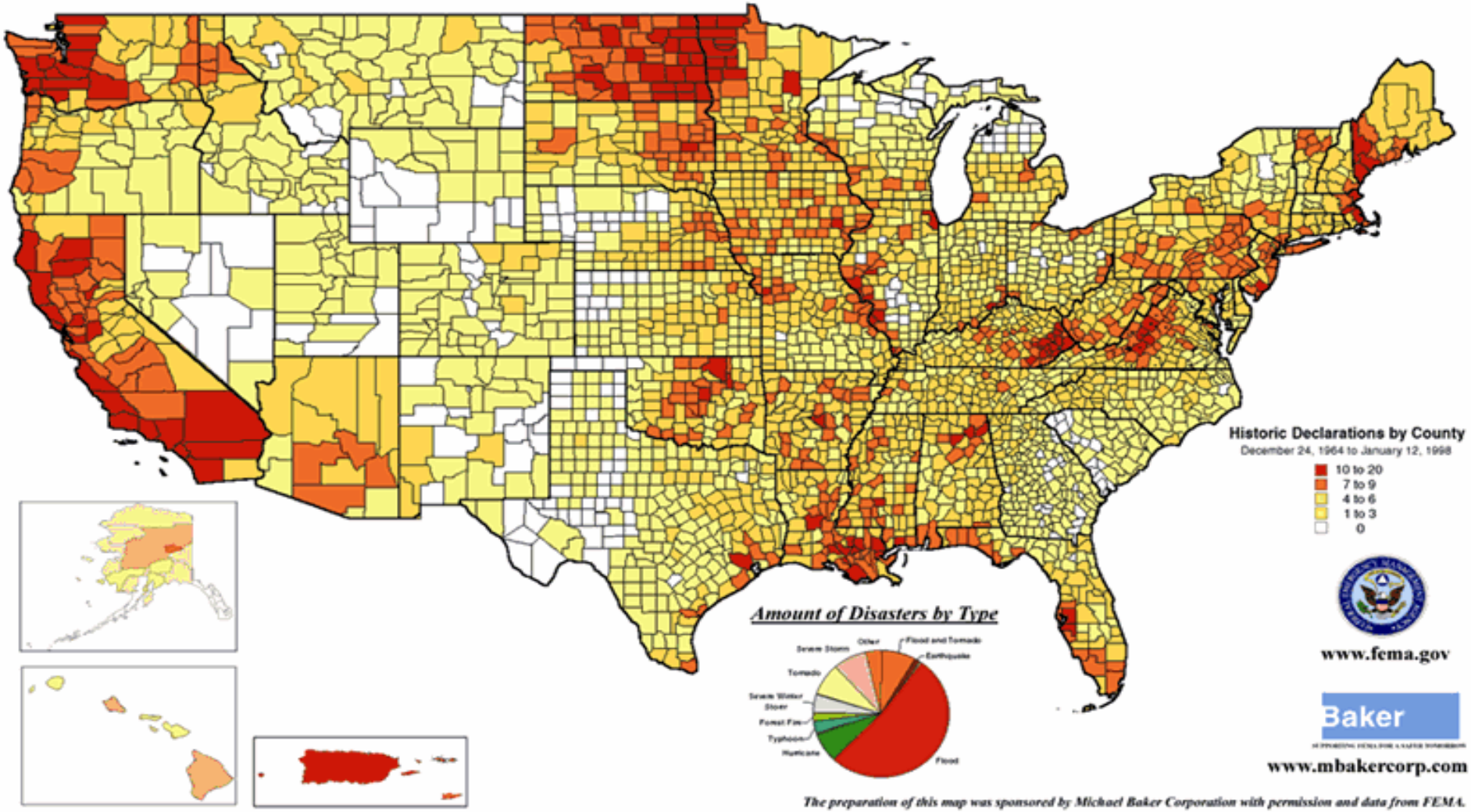
ecfirst.com
HEALTHCARE

Wireless Challenges

- **Lack of user authentication**
- **Weak encryption**
- **Poor network management**
- **Vulnerable to attacks:**
  - Man-in-the-middle
  - Rogue access points
  - Session hijacking
  - DoS

HISTORICAL PRESIDENTIAL DISASTER DECLARATIONS

1,198 DECLARATIONS SINCE 1964



The preparation of this map was sponsored by Michael Baker Corporation with permission and data from FEMA.

"To successfully mitigate against disaster will require the combined talents and concerted efforts of all levels of government, academia, professional and voluntary organizations, the corporate sector, and all Americans."

- Bill Clinton, December 6, 1995

Typical Security Remediation Initiatives

Typical Priorities

- Deploy Firewall Solutions, IDS/IPS
- Secure Facilities & Server Systems
- Deploy Device & Media Control Solutions
- Implement Identity Management Systems
- Deploy Single Sign-On (SSO) and Context Management Solutions
- Implement Auto-logoff Capabilities
- Deploy Integrity Controls and Encryption
- Activate Auditing Capabilities
    - Both system as well as record access
- Test Contingency Plans
- Update Security Policies
- Security Training & Awareness

ecfirst.com
HEALTHCARE

Contingency Plan

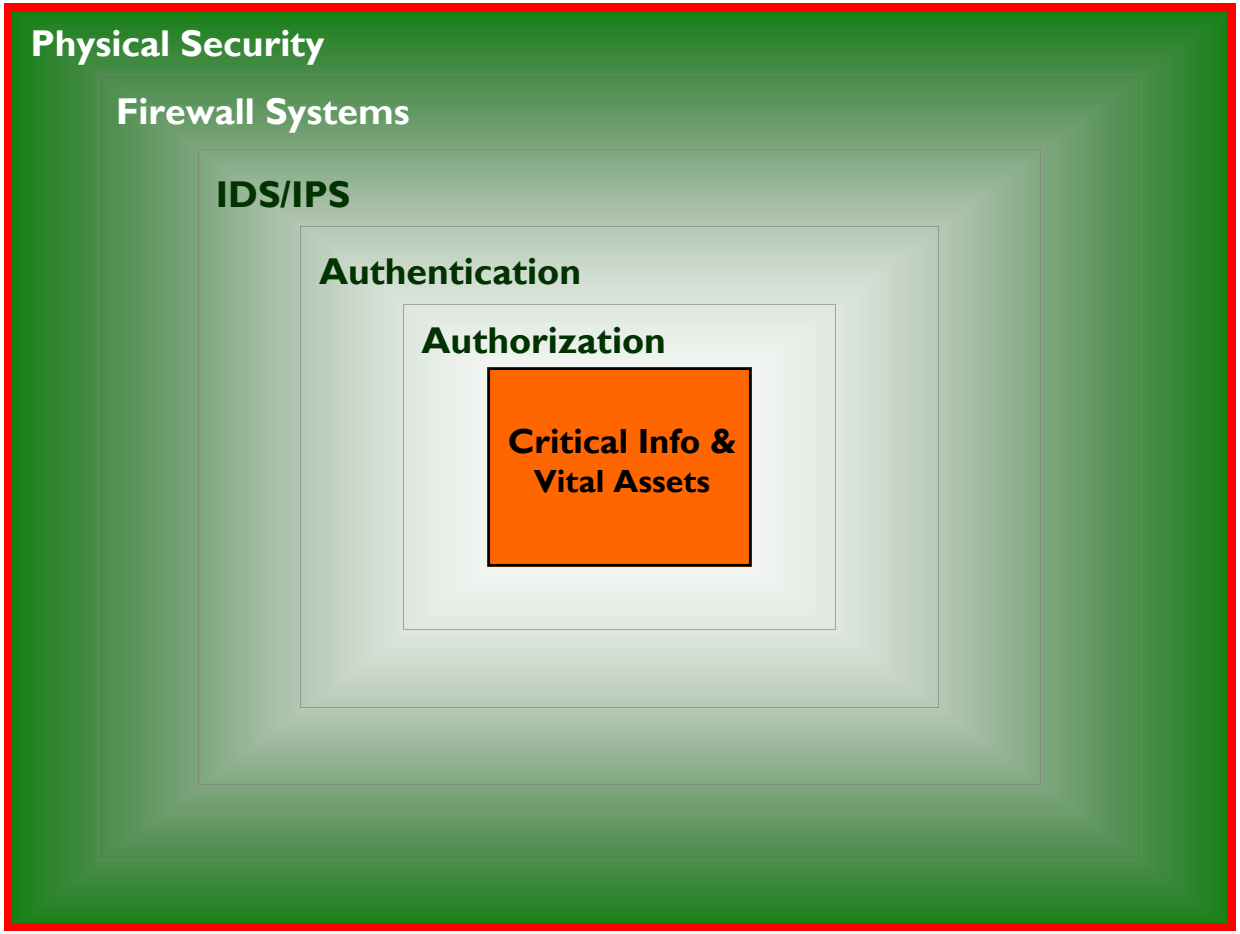
- It is a U.S. Federal law that must be met
- For example, the HIPAA Security Rule Standard that includes:
  - Data Backup Plan (R)
  - Disaster Recovery Plan (R)
  - Emergency Mode Operation Plan (R)
  - Testing and Revision (A)
  - Applications and Data Criticality Analysis (A)
- Requirements also further identified under Physical and Technical Safeguards

ecfirst.com
HEALTHCARE

Critical Steps

ecfirst.com HEALTHCARE

Defense In-Depth



ecfirst.com
HEALTHCARE

Information Security Posture?

- State of information security in business today:
  - Information security executives have more information than ever – but that does not mean they know what to do with it
  - The bigger the organization the more it watches its employees
    - Dramatic rise in surveillance (tracking workers information access)
      - Want to rein in instant messaging and other applications
  - Security executives still have difficulty:
    - Identifying who is attacking them
    - Where the attack is coming from
    - How the attack is being executed
  - Firewalls/log files/IDS are typically the way attacks are discovered
- **Compliance establishes minimal capabilities to deter and detect attacks**

ecfirst.com HEALTHCARE

Recommendations

ecfirst.com
HEALTHCARE

Technology Architecture

- "Thin is In"
- Bring the complexity to the data center
- Reduce the number of servers
  - Virtualization
  - Blade servers
- Plan for multi-tier storage architecture
- In new acquisitions, bake in:
  - Security
  - Compliance
  - Redundancy

ecfirst.com
HEALTHCARE

Enterprise Security Goals

Establish your enterprise security objectives.

These may include:

1. Ensure confidentiality, integrity & availability of all sensitive business information
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of information
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
4. Ensure compliance with legislations and standards as required

ecfirst.com
HEALTHCARE

Compliance Requirements & Investment

- Identify the security official to lead security and compliance initiatives
- Conduct an accurate and thorough assessment of the potential risks to sensitive information
- Develop policies and implement a security awareness and training program for all members of the workforce
- Establish IT capability for contingency planning and disaster recovery
- Perform periodic audit and evaluations to determine compliance status

Investment typically required for a "mid-size" healthcare organization ~ $150,000/year

ecfirst.com
HEALTHCARE

What is Your Strategy?

"The true organization is so prepared for battle that battle has been rendered unnecessary."

"Much strategy prevails over little strategy, so those with no strategy cannot but be defeated (defenses penetrated). Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win."

Sun Tzu
The Art of War

Critical for organizations to seriously develop their strategy first, then execute.

ecfirst.com
HEALTHCARE

Thank You!

For a complimentary copy of **Get Compliant. Get Secure!,** email your testimonial to:

E: **Pabrai@ecfirst.com**

P: 949.260.2030

ecfirst.com HEALTHCARE