Contingency Planning

Drew Hunt
Network Security Officer
Valley Medical Center

About me

- M.Ed., CISSP, MCT
- Technical geek
- HIPAA Advocate
- Developed and taught Information Assurance courses for the Department of Defense
- Visited by Aliens in 1992

Why a Contingency Plan?

- Types of Disasters
  - Natural Disasters
  - Accidental Disasters
  - Intentional Disasters
- 65 % of businesses that cannot recover from a disaster within a week go out of business permanently
- Garner Group expects that 1/3 of US businesses are not prepared for major disaster.

Natural Disasters

- Seattle Earthquake in 2000 cost 2.0 billion dollars
- Hurricane Andrew (FL, LA) in 1992 cost $1.8 billion dollars
- Midwest Floods (IL, IA, KS, MN, MO, NE, ND, SD, WI) in 1993 $1.1 billion dollars
- LA quake in 1994 caused $15.3billion dollars of damages.

Accidental Disaster

- Data losses cost businesses 11.8 billion dollars in 1998.
- Estimated that 3% of disasters were by natural causes while 32% disasters were caused by human error.

Intentional Disasters

- Viruses
  - Sobig.f fastest virus in history
    - Grounded Air Canada, Lockheed Martin
  - Slammer Worm
  - SuperWorm?
- Theft
  - Tri-West lost 550,000 medical records
  - Hacker gained access to UW Medical Center

HIPPA Contingency Plan

- Referenced in CFR 164308(a)(7)
- Defined as polices and procedures for responding to an emergency or disaster

Contingency Plan Implementation Specifications

- Required Specifications:
  - Data backup plan
  - Disaster recovery plan
  - Emergency mode operation plan
- Addressable Specifications:
  - Testing and revision procedures
  - Applications and data criticality analysis

Data Backup

- Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information
- Test and practice restoring from backup
- Consider off site storage

Disaster Recovery Plan

- Primary goal of a disaster recovery plan is to minimize the effects of a disaster.
- Establish procedures to restore any loss of data.

Emergency mode operation plan

- Establish procedures to secure electronic protected health information while operating in emergency mode.
- Identify critical business processes

Testing and Revision Procedures

- Implement procedures for periodic testing and revision of contingency plans.
- Consider employee turnovers, infrastructure changes, hardware and software changes, etc…

Applications and Data Criticality Analysis

- Assess the relative criticality of specific applications and data in support of other contingency plan components.
- Identify resources and subsystems that support critical functions such as, patient scheduling, billing, payroll, and patient care services.

Questions