**HARDWARE AND SOFTWARE RISK ANALYSIS EXAMPLES**

**Possible Vulnerability sources** **Risk REMEDIES**

|  |  |  |
| --- | --- | --- |
| Natural Threats:  1. Earthquakes 2. Landslides 3. Storm Damage (ice, snow, floods) 4. Tornadoes, hurricanes | Low Low Medium High | Emergency Access, Back Up  Emergency Access, Emergency Operation Plan, Data Integrity, Backup, Disaster Recovery Plan (Covers threats 1, 3 and 4) |
| Environmental Threats:  1. Fire and smoke contamination 2. Building collapse or explosion 3. Power (blackouts, spikes, surges) 4. Utility problems (HVAC) 5. Broken or leaking water, sewer, or natural gas lines 6. Toxic materials release 7. Contagious disease epidemic | Medium Low Medium Medium Low Low Low | Emerg Access, Emerg Op Plan, Backup  Backup, Data Integrity Backup, Data Integrity |
| Human Threats:  1. Accidental Acts 2. Input errors and/or omissions 3. Faulty programming/processing 4. Phone or network cable broken 5. Inappropriate Activities 6. Inappropriate content 7. Waste of practice resources 8. Harassment 9. Abuse of privileges or rights 10. Workplace violence 11. Illegal operations/ intentional attacks 12. Eavesdropping 13. Snooping 14. Fraud 15. Theft 16. Vandalism 17. Sabotage 18. Extortion 19. External attacks (virus/hacking) 20. Other acts 21. War 22. Labor strikes | Medium  Medium  Medium  Low | Unique User ID, Access Contr, Audit Contr  Unique User ID, Access Contr, Audit Contr  Unique User ID, Access Contr, Audit Contr |

## **Hardware and Software Remedies**

1. Unique User ID 7. Access Controls

2. Emergency Access

3. Automatic Logoff 8. Audit Controls

4. Authentication 9. Data Integrity

5. Encryption 10.Backup

6. Emergency Operation Plan 11.Disaster Recovery Plan