Incident Planning Guide: Information Technology (IT) Failure

Definition

This Incident Planning Guide is intended to address information technology (IT) incidents including, but not limited to, server security breach, server virus infection, communications failure, solar flare, or an electromagnetic pulse disrupting electronic equipment. Hospitals may customize this Incident Planning Guide for their specific requirements.

Scenario

Information technology assessments at your hospital indicate that about 80% of the systems are updated weekly with the latest patches and firewalls, but some systems are months out of date and, for a few, years out of date. Late last evening, all printers throughout your hospital begin to print reams of gibberish. This morning, there are widespread computer associated problems: computers are slow to boot up; are not loading; and are filling up with pornography. The Chief Information Officer received an email from someone claiming to have invaded the system using a Trojan horse program and threatened to broadcast the patient information database unless he's paid at least $4 million. System administrative passwords are compromised. Email is not available. Servers are shut down and unable to reboot. Router traffic is unreliable. The internal phone system and computers used for patient monitoring are unreliable (data displays show altered information and alarms switch off by themselves). System surveys indicate that 90% of patient records in the system may have been compromised. The Chief Information Technology Officer's assessment is that with consultant support, he can sterilize and return to use about 75% of computers used for documentation and order entry in two days. Unfortunately, the computer based patient monitoring systems will remain unreliable for longer. Email servers and router traffic will also remain unavailable for at least two days. Backup tapes have been contaminated over the previous 2 months. As the news of these events spreads, there is great interest from local licensing and certification authorities, media, and social media.

Does your Emergency Management Program address the following issues?

Mitigation	
1.	Does your hospital address the threat and impact of an information technology (IT) failure in the annual Hazard Vulnerability Analysis, including the identification of mitigation strategies and tactics, and a system-wide business impact analysis of all critical and non-critical IT systems?
2.	Does your hospital have: ☐ The latest versions of firewall, antivirus, and spyware software technologies deployed across the enterprise? ☐ A system to monitor misuse or unauthorized remote access of cybersystems, especially by personnel with access to major data and system integrity? ☐ A proactive and well documented cybersecurity training program for all personnel with potential access? ☐ Rules and remote filters for employees working from home to comply with information and systems security?
3.	Does your hospital complete a Hazard Vulnerability Analysis of all cybersystems to determine infrastructure security risks and identifed improvements needed for all internal and external threats?
4.	Does your hospital have the ability to terminate access immediately upon an employee's termination of employment?
Preparedness	
1.	Does your hospital have an Information Technology Failure Plan that includes enhanced awareness training for staff?
2.	Does your hospital exercise the Information Technology Failure Plan annually and revise it as needed?
3.	Does your hospital include preparedness strategies to reduce the impact from an information technology failure in your emergency management program annual goals?
4.	Does your hospital establish criteria and procedures to activate a Hospital Command Center during emergencies, including who has the authority to activate the plan?
5.	Does your hospital have a Communications Plan that includes: ☐ Working with the Joint Information Center in cooperation with local, regional, and state emergency management partners? ☐ Use of social media for communication, including: o Who can use social media? o Who approves the use of social media? o When is use of social media not appropriate? ☐ Procedures for notification of internal and external authorities (local, county, region, state)? ☐ A plan to distribute radios and auxiliary phones to appropriate people and hospital areas? ☐ A plan for rapid communication of situation status to local emergency management and area hospitals?

6.	Does your hospital have: ☐ An information technology system malfunction alert and notification procedure? ☐ Trained personnel for information technology response and recovery operations? ☐ Standards for the development and security of systems and substructures (i.e., departments), including non information systems staff with special levels of cybersystems knowledge? ☐ Policies for the interface and deployment of wireless data and voice systems communications? ☐ Backup or alternate contingencies in place for communications, network failure, or equipment failure? ☐ Data backup and data redundancy processes and policies for enterprise wide and departmental specific data systems, including testing to ensure backups are functional? ☐ Data security exchange protocols for secure interface with authorized emergency management agencies? ☐ A management process to approve all information technologies utilized in the organization including, but not limited to, different systems sharing like data and how shared or exchanged data is protected from corruption while allowing access to critical data under emergent conditions? ☐ A protocol to monitor the number of cybersystem response incidents involving external attacks by deliberate attempts to penetrate security and to take appropriate protective actions? ☐ A system of cyber security audits using a scenario based evaluation or a series of critical benchmarks approved by a multidisciplinary committee within your organization? ☐ Policies and procedures for notification of patients and appropriate officials in the event of a protected health information breach? ☐ Departmental Business Continuity Plans with clear recovery time objectives in place? Are these plans tested and exercised?
7.	Does your hospital comply with current standards on disaster and emergency management and business continuity as they apply to all third party vendors that support and supply cyber technology services, such as offsite backup and data recovery processes?
8.	Does your hospital comply with current standards on disaster and emergency management and business continuity as they apply to all third party vendors that support and supply cyber technology services, such as offsite backup and data recovery processes?
Immediate and Intermediate Response	
1.	Does your hospital have: ☐ Systems and procedures to determine what information technology systems are affected by the incident? ☐ Procedures to obtain information on possible entry points of an information technology failure incident? ☐ Procedures to evaluate firewall management and containment, and to respond accordingly? ☐ Policies for the Chief Information Officer or Information Technology Manager to direct staff in identifying potential problem areas?

2.	Does your hospital have communication methods to: ☐ Issue organizational alerts regarding information technology system failures or viruses affecting systems? ☐ Determine contact lists and communication methods to immediately notify nursing staff and senior medical staff regarding affected information technology systems that will have direct impact on healthcare delivery and the potential to adversely affect patient safety? ☐ Provide emergency incident notification when affected systems will take a significant amount of time to return to full operational status and to alert the Incident Commander and disaster recovery personnel? ☐ Notify patients regarding any delays in service and the overall situation? ☐ Implement regular briefings on information technology systems restoration status for personnel?
3.	Does your hospital have procedures for all administrators and healthcare delivery staff to use manual documentation systems or unaffected portable devices and later merge data with recovered systems?
4.	Does your hospital have procedures to identify critical systems and operations directly impacted by a cybersystem compromise (e.g., medical care, patient records, admissions, finance, supply management, computer aided hospital management)?
5.	Does your hospital have procedures to ensure resources (i.e., personnel, equipment, software, and hardware) are obtained as appropriate to provide the fastest and most secure level of information systems recovery?
Extended Response and System Recovery	
1.	Does your hospital have a Business Continuity Plan for long term events?
2.	Does your hospital have Hospital Incident Management Team position depth to support extended operations?
3.	Does your hospital have criteria to restore normal information technology operations?
4.	Does your hospital have procedures to complete incident documentation and archiving?
5.	Does your hospital have a continuing process to capture all costs and expenditures related to operations?
6.	Does your hospital have a plan to provide behavioral health support and stress management debriefings to patients, staff, and families, including obtaining services of local or regional resources?
7.	Does your hospital have 24/7 access to risk management and legal counsel?
8.	Does your hospital have procedures to collect and collate incident documentation and formulate an After Action Report and Corrective Action and Improvement Plan for submission to the Incident Commander?