CYBER ATTACK

SCENARIO

A disgruntled former hospital employee with exceptional computer skills hacks into the hospital network from their home computer and plants a very aggressive computer virus into the Computer-Aided Facility Management (CAFM) system.

The computer virus activates at midnight, shutting down the hospital HVAC system, security system, building automation, and patient medical monitoring system.

CYBER ATTACK

INCIDENT PLANNING GUIDE

Does your Emergency Management Plan Address the following issues?

Mitigation & Preparedness

1.	Does your hospital have the latest versions of firewall, anti-virus, and spyware software technologies deployed across the enterprise?
2.	Does your hospital have a system to monitor misuse or unauthorized/remote access of cyber-systems, especially by personnel under emotional or financial strains and with access to major data and system integrity?
3.	Does your hospital have a proactive and well-documented cyber-security training program for all personnel with potential access?
4.	Does your hospital have rules for employees working from home to comply with information and systems security?
5.	Does your hospital have data back-up (data redundancy) processes and policies for enterprise wide and departmental specific data systems?
6.	Does your hospital have a management process to approve all cyber-technologies utilized in the organization, including but not limited to different systems sharing like data and how shared or exchanged data protected from corruption while allowing access to critical data under emergent conditions?
7.	Does your hospital have policies for the interface and deployment of wireless data and voice systems communications?
8.	Does your hospital have trained personnel for cyber-system response and recovery operations?
9.	Does your hospital have a protocol to monitor the number of cyber-system response events involving external attacks by deliberate attempts to penetrate, and take appropriate protective actions?
10.	Has your hospital completed a hazard vulnerability analysis of all cyber-systems to determine infrastructure security improvements needed for all internal and external threats?
11.	Does your hospital have data security exchange protocols for secure interface with authorized emergency management agencies under a unified command?
12.	Does your hospital comply with current standards on disaster/emergency management and business continuity programs as they apply to all third-party vendors that support and supply cyber-technology services, such as offsite backup and data recovery process for the institution?
13.	Does your hospital have a system of cyber-security audits using a scenario based evaluation or a series of critical benchmarks approved by a multi-disciplinary committee of your organization?
14.	Does your hospital have standards for the development and security of systems and substructures (i.e., departments), including non-IT/IS staff with special levels of cyber-systems knowledge?
15.	Does your hospital have the ability to terminate access immediately upon an employee's termination of employment?

CYBER ATTACK

INCIDENT PLANNING GUIDE

Response & Recovery	
1.	Has you hospital established criteria and procedures to activate an IT/IS command center (partial or complete) during emergencies?
2.	Does your hospital have systems and/or procedures to determine what cyber-systems are affected by certain events?
3.	Does your hospital have procedures to obtain information on possible entry point of cyber-security violation?
4.	Does your hospital have procedures to evaluate firewall management and containment and to respond accordingly?
5.	Does your hospital have policies for the CIO or IT/IS manager to direct key IT/IS staff in identifying potential problem areas?
6.	Does your hospital have communication methods for the CIO or IT/IS manager to issue organizational alerts regarding cyber-systems failures or viruses affecting systems?
7.	Does your hospital have the ability to determine contact lists and communications methods in order for the CIO or IT/IS manager to immediately notify nursing staff (nursing house supervisor) and/or senior medical staff (chief of staff) regarding affected cyber-systems that will have direct impact on health care delivery and potential to adversely affect patient safety?
8.	Does your hospital have procedures for emergency incident notification when affected systems will take greater than two hours to return to full operational status, to alert the Incident Commander and key disaster response personnel?
9.	Does your hospital have procedures for all administrators and key health care delivery staff to use manual documentation systems or non-affected portable devices and later merge data with recovered systems?
10.	Does your hospital have procedures to identify medical care, patient records, admissions, financial, supply management, computer aided facility management (CAFM), and other critical systems and operations directly impacted by cyber system compromise?
11.	Does your hospital have a plan to notify patient about any delays in service and the situation?
12.	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 cyber-systems recovery?
13.	Does your hospital have procedures to implement regular briefings on cyber-system restoration status for personnel?
14.	Does your hospital have pre-developed, departmental business continuity plans with clear recovery time objectives (RTOs) in place. Are these plans practiced?
15.	Does your hospital have criteria to restore normal operations?
16.	Does your hospital have procedures to complete incident documentation and archiving?

17.	Does your hospital have procedures to debrief staff and identify corrective actions?
18.	Does your hospital identify components to include in an After Action Report, including a cost analysis of time spent of restoration efforts?
19.	Does your hospital have procedures to revise the Emergency Operations Plan as needed, including enhanced staff awareness training?

CYBER ATTACK

INCIDENT RESPONSE GUIDE

Mission: To ensure business continuity and availability of essential automated systems for the clinic/hospital/health care system in the event of a massive or sustained cyber-systems compromise or attack.

Directions

- ☐ Read this entire response guide and review incident management team chart
- ☐ Use this response guide as a checklist to ensure all tasks are addressed and completed

Objectives

- ☐ Define scope of problem
- ☐ Isolate affected systems
- ☐ Restore automated systems and services
- ☐ Notify affected end-user supervisory personnel and provide directed guidance on systems use

Immediate Actions (Operational Period 0-2 Hours)

COMMAND

(Incident Commander):

- ❑ Activate the IT/IS Unit Leader to assess the degree of cyber-systems intrusion or disruption
- ❑ Activate appropriate Command Staff and Section Chiefs

(PIO):

- ❑ Prepare initial risk communications for staff and patients regarding the cyber-systems situation and recommended actions until the systems are restored

☐ (Liaison Officer):

- ❑ Work with the Incident Commander and senior IT/IS staff to determine if the disruption is deliberate and targeted; contact local law enforcement, the FBI Cyber-Terrorism Division, and state Cyber-Terrorism Division or District Office, as appropriate
- ❑ Notify local emergency management authority, if appropriate

(Safety Officer):

- ❑ Ensure the safety of staff, patients and visitors in areas impacted by the automated system shut downs
- ❑ Ensure safe restoration of services and systems

CYBER ATTACK

INCIDENT RESPONSE GUIDE

OPERATIONS

- ❑ Activate the Business Continuity Branch Director to isolate affected systems and develop a severity of impact list to begin to establish restoration priorities in accordance with the business continuity plan
- ❑ Conduct a risk assessment regarding any automated environmental systems that may be affected and alternate plans to provide HVAC and other critical facility services in direct support of health care operations.

☐

- ❑ Notify key staff including house supervisors, chief of staff, Business Continuity Branch Director, support services, and others designated in the business continuity plan as it applies to cyber-systems disruptions
- ❑ Ensure continuation of patient care and management activities
- ❑ Ensure security of the facility
- ❑ Implement procedures to provide manual environment controls (HVAC systems are down)
- ❑ Activate redundant/back up documentation systems
- ❑ Consider need for patient evacuation or relocation in the facility due to loss of essential services

PLANNING

☐

- ❑ Establish operational periods, incident objectives and develop Incident Action Plan, in collaboration with the Incident Commander
- ❑ Implement manual documentation systems until automated systems can be restored

LOGISTICS

☐

- ❑ Activate IT/IS Unit Leader and personnel to isolate affected systems and develop a severity of impact list to begin to establish restoration priorities in accordance with the business continuity plan
- ❑ Implement redundant communications and reporting mechanisms as necessary

CYBER ATTACK

INCIDENT RESPONSE GUIDE

Intermediate (Operational Period 2-12 Hours)

COMMAND

(Incident Commander):

- ❑ Conduct regular briefing and situation updates with Command Staff and Section Chiefs
- ❑ Update and revise the Incident Action Plan

(PIO):

☐
- ❑ Establish a central information center (clearinghouse) as needed to address all staff or patient issues that may arise as result of a cyber-systems disruption

(Liaison Officer):

- ❑ Continue to update local emergency management and other officials on situation and hospital status

(Safety Officer):

- ❑ Conduct ongoing analysis of existing response practices for health and safety issues related to staff, patients, and facility, and implement corrective actions to address

OPERATIONS

- ❑ Reassess HVAC and other critical services in direct support of healthcare operations and modify actions as necessary

☐
- ❑ Reevaluate need to transfer or relocate patients to ensure safety
- ❑ Continue the patient care and management and identify any patient care systems that are affected during the course of the restoration process
- ❑ Continue to assess cyber-systems disruptions and revise cyber security response plan

PLANNING

☐
- ❑ Update and revise the Incident Action Plan
- ❑ Initiate patient and bed tracking if patients are evacuated or relocated within the facility

LOGISTICS

☐
- ❑ Provide alternate documentation systems and support hardware (i.e., providing laptops and printers to affected areas for temporary use until systems are fully restored)

CYBER ATTACK

INCIDENT RESPONSE GUIDE

FINANCE/ADMINISTRATION

☐

- ❑ Track cost of response and restoration activities and expenditures
- ❑ Monitor and track costs related to the disruption to business continuity and compromise of automated systems

Extended (Operational Period Beyond 12 Hours)

COMMAND

(Incident Commander):

- ❑ Continue regular meetings and briefings with Command Staff and Section Chiefs to determine situation status and timelines for restoration of services

(PIO):

☐

- ❑ Update staff, patients and visitors on the situation status

(Liaison Officer):

- ❑ Continue to update local emergency management on situation status
- ❑ Notify appropriate licensing authorities of the sentinel event, as appropriate, in coordination with the Incident Commander

PLANNING

☐

- ❑ Update and revise the Incident Action Plan
- ❑ Track personnel, patients and beds as necessary

LOGISTICS

☐

- ❑ Monitor computer systems for new cyber-threats if the corrective actions are not completed within two hours

CYBER ATTACK

INCIDENT RESPONSE GUIDE

Demobilization/System Recovery

COMMAND

(Incident Commander):

- ❑ Ensure full system recovery and return to normal operations
- ❑ Declare the incident terminated

☐ (PIO):

- ❑ Issue final media update with hospital status and appropriate service disruption information, in collaboration with the Incident Commander

(Liaison Officer):

- ❑ Notify local emergency management of system recovery and incident termination

OPERATIONS

- ❑ Restore patient care to normal operations
- ❑ Repatriate patients, if evacuated or transferred to other areas within the hospital
- ❑ Restore infrastructure services
- ❑ Prepare a summary report of corrective actions and recommendations for updating/improving diagnostic and protective cyber-services

PLANNING

- ❑ Write after-action report and improvement plan including the following:
  - Summary of actions taken
  - Summary of the incident
  - Actions that went well
  - Area for improvement
  - Recommendations for future response actions
  - Recommendations for correction actions

☐

Documents and Tools

☐	Hospital Emergency Operations Plan
☐	Hospital and Department Level Business Continuity / Business Recovery Plan
☐	Manual procedures for System Downtime

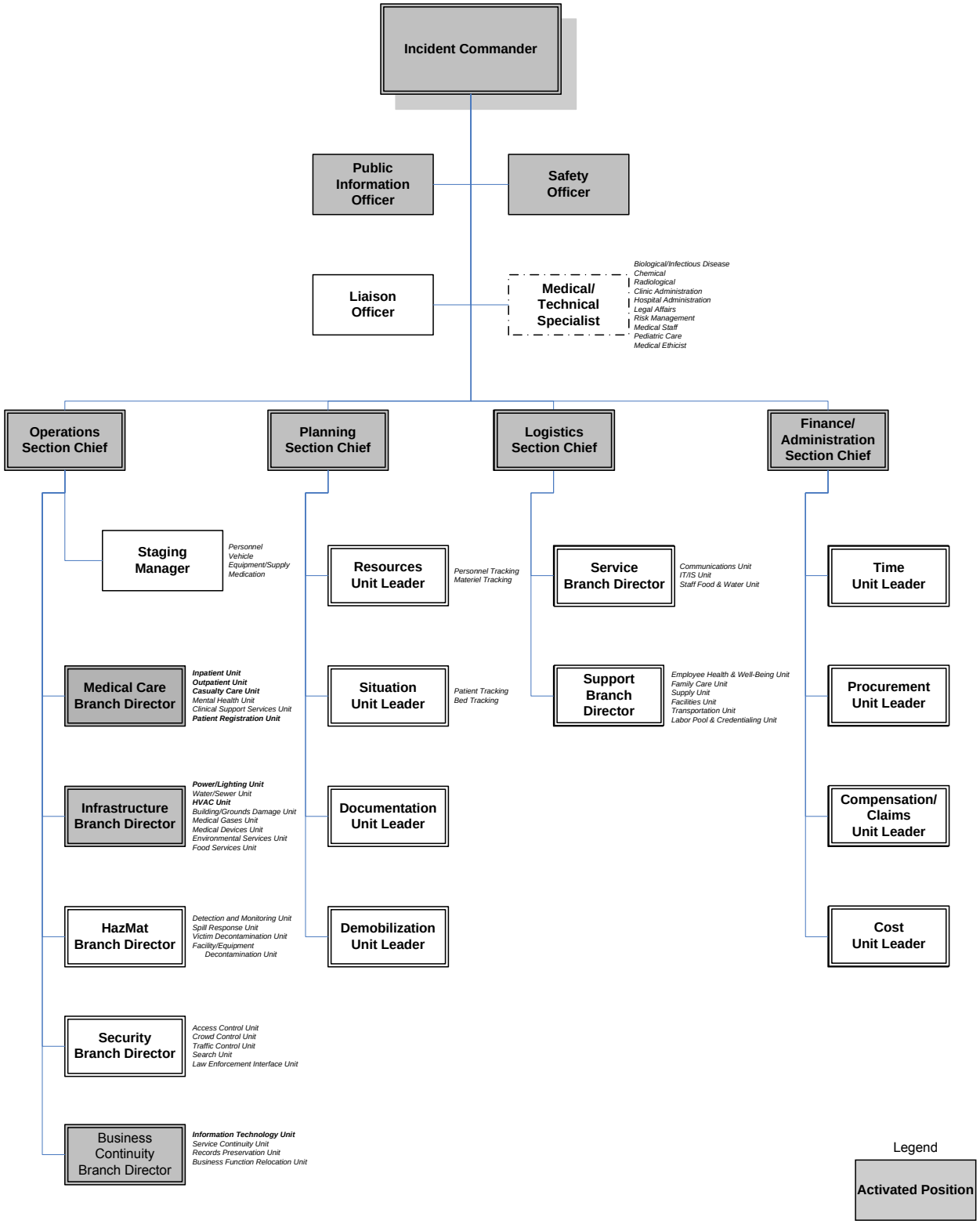
CYBER ATTACK

INCIDENT RESPONSE GUIDE

☐	Cyber-Systems Diagnostics (e.g., anti-virus, spyware, firewall software systems)
☐	Cyber-systems Malfunction Alert Notification

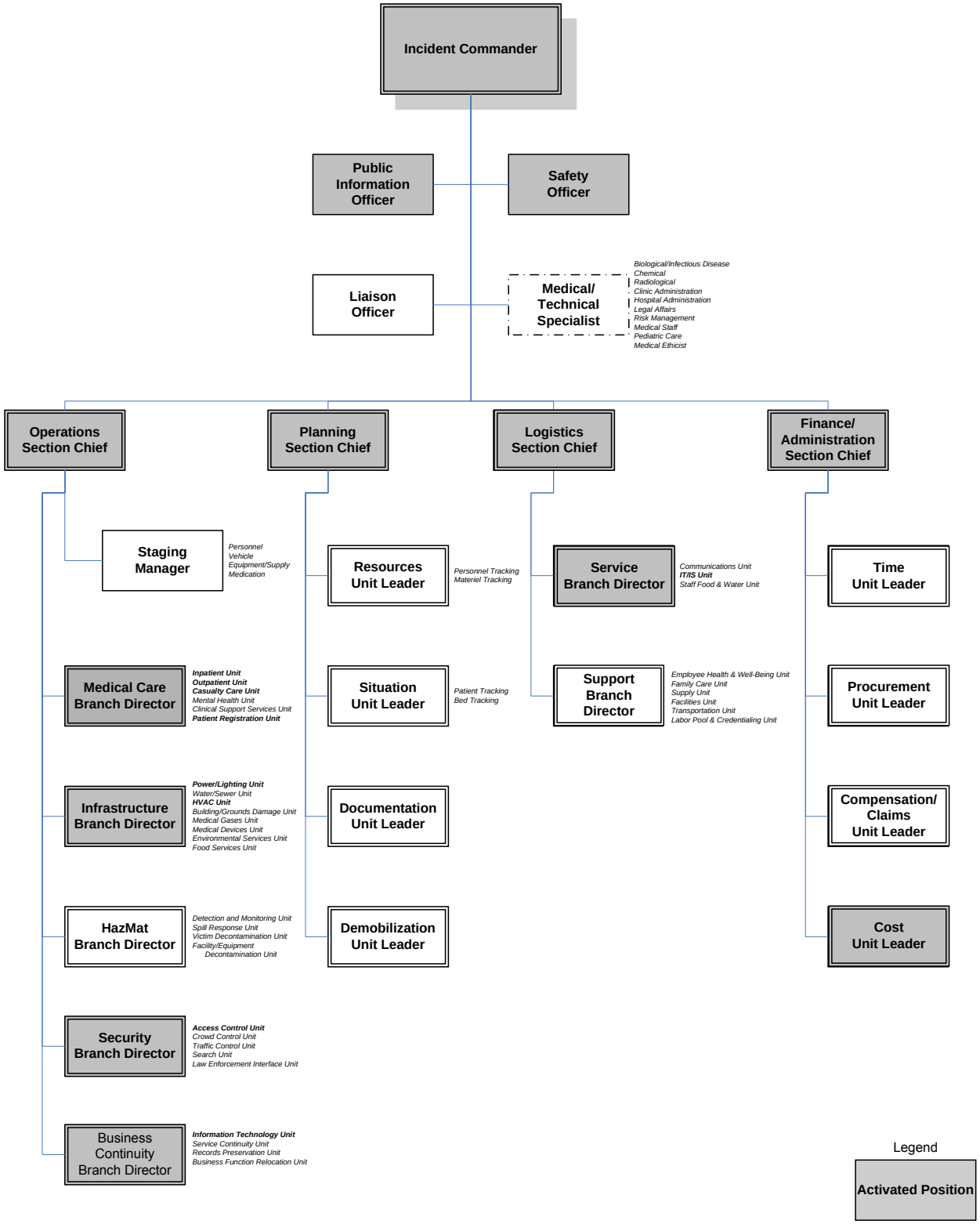
CYBER ATTACK

INCIDENT MANAGEMENT TEAM CHART – IMMEDIATE



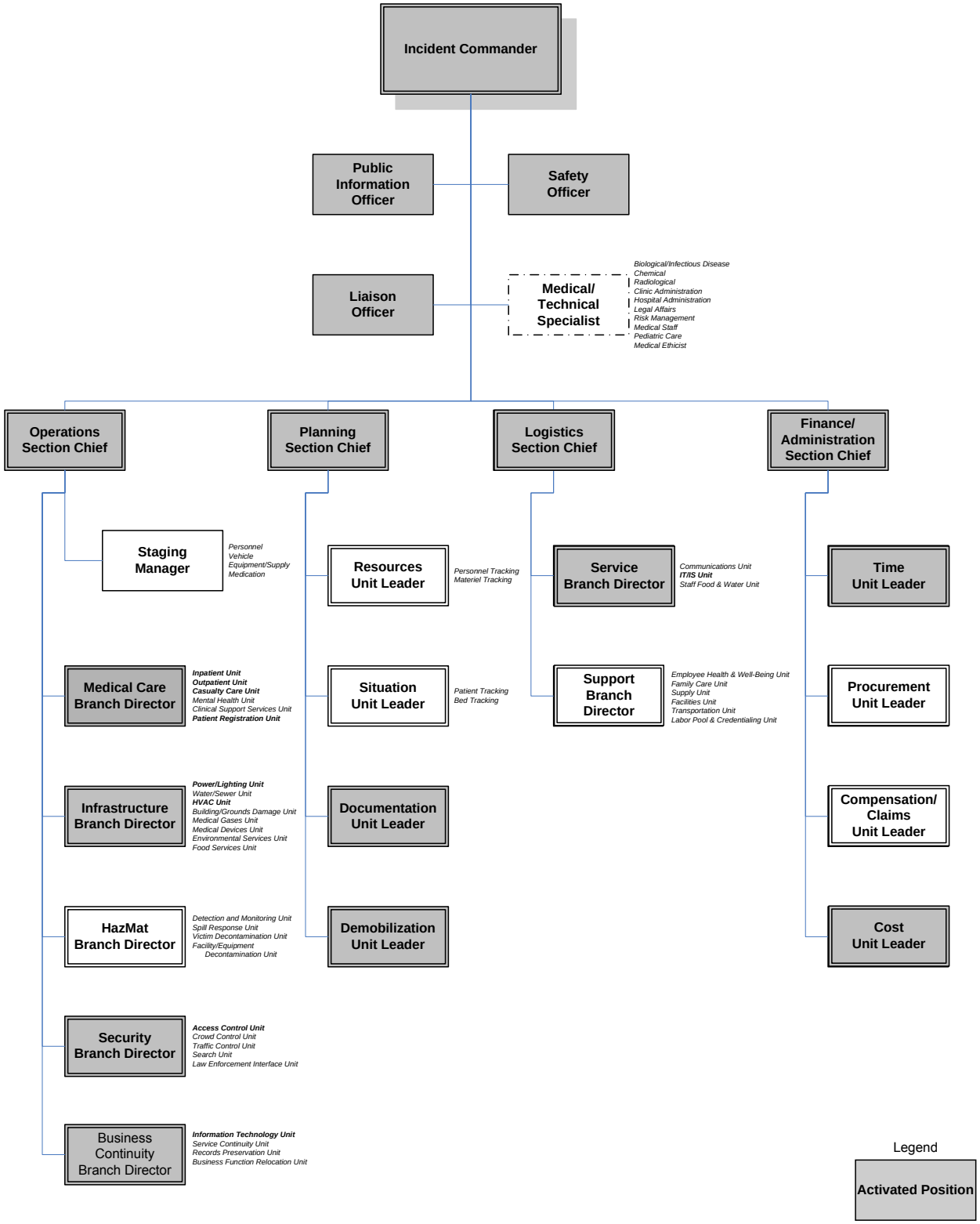
CYBER ATTACK

INCIDENT MANAGEMENT TEAM CHART – INTERMEDIATE



CYBER ATTACK

INCIDENT MANAGEMENT TEAM CHART – EXTENDED



CYBER ATTACK

INCIDENT MANAGEMENT TEAM CHART – DEMOBILIZATION