APPENDIX: CYBER-ATTACK RESPONSE PROCEDURES TEMPLATE

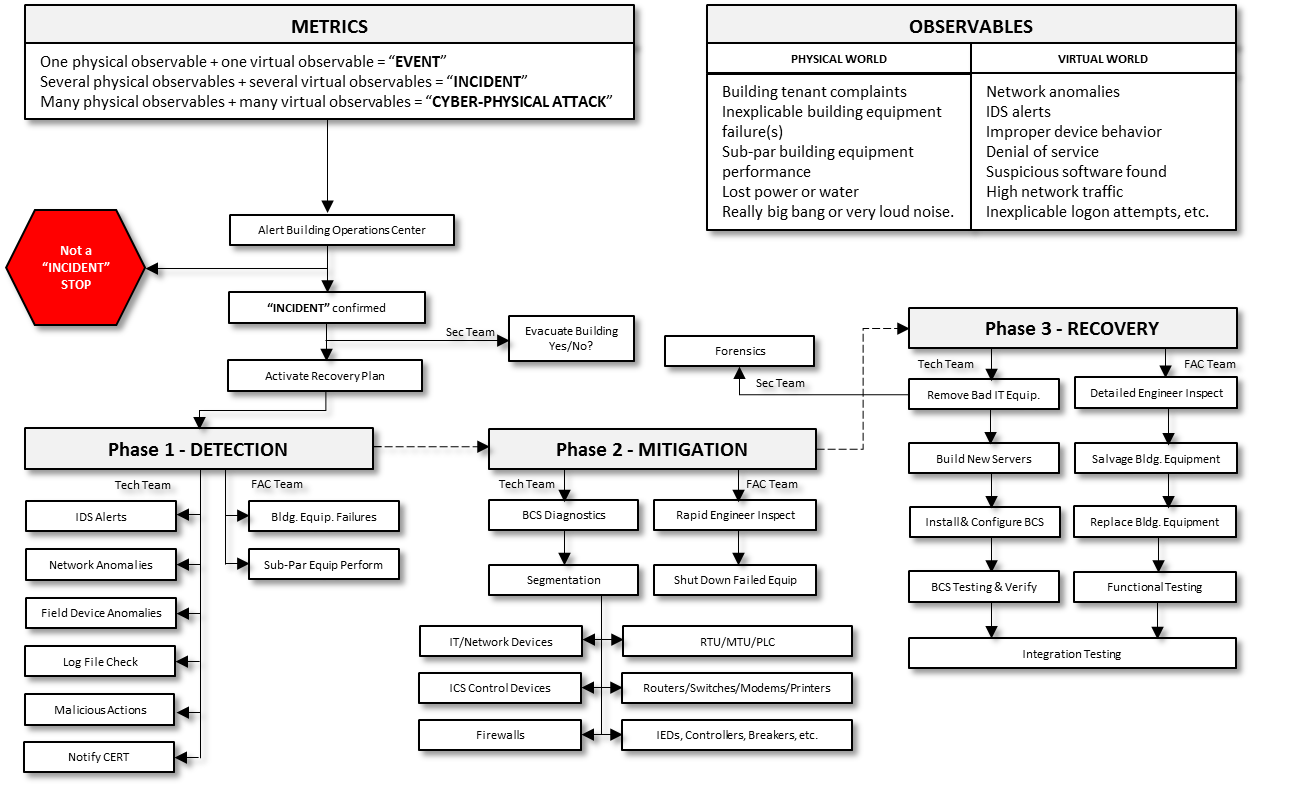
Soft copy of these forms (fully editable with fillable fields) is available for download from www.apress.com/9781484221549.

**<<Facility Name>>**

**<<Date Prepared>>**

**<<Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_>>**

**<<Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_>>**



Cyber-Attack Response Procedures Flow Chart

# HOSPITAL CYBER-ATTACK RESPONSE PROCEDURES

The following forms can be downloaded and customized to create your own Cyber-Attack Response Plan. Each form includes a brief description of the form, why the form is needed, who should fill out the form and how often the form should be updated.

# Intrusion Detection System Alerts

An Intrusion Detection System (IDS) is a hardware or software product that gathers and analyzes information from various areas within a computer network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)

An IDS alerts us whenever it detects suspicious behavior such as any of the following:

* Unauthorized user logging in
* Virus or Trojan horse detected
* Rapid and/or continuous log-ins/log-outs
* Users logging into accounts outside of normal working hours
* Numerous failed log-in attempts
* User accounts attempting to escalate account privileges
* Suspicious software and/or configurations on a server or workstation
* Unusual system behavior
* Irregular process found
* Spontaneous reboots or screen saver change
* Unusually slow performance or usually active CPU
* CPU cycles up and cycles down for no apparent reason
* Intermittent loss of mouse or keyboard
* Configuration files changed without user or system administrator action in operating system
* Configuration changes to software made without user or system administrator action
* Network unresponsive
* When an asset is communicating outside the bounds of the data flow baseline
* HMI, OPC, and controllers not synchronized
* Unexpected changes to instructions, function calls, commands, or alarm thresholds being sent from HMI or OPC to controllers
* HMI or OPC not updating after operator made changes to instructions, commands, or alarm thresholds
* Expected changes to controllers are not appearing on controllers
* An irregular vendor patch coming from an external source, or unexpected source, to a device within the network
* A device on the network is communicating with an undocumented, unauthorized, or unknown IP address
* A device other than authorized devices is sending field controller traffic to a network device
* Traffic coming or going to an unknown device
* A field controller is communicating with an unknown device
* A medical device has expanded its communications to other devices within the network

As you can see, there are many “observables” that tell us something is going on that we need to explore. Many alerts are not malicious and may be due to authorized events or can otherwise be explained:

* Was maintenance performed on the equipment or a software update installed recently?
* Did the equipment simply malfunction?
* Did the equipment lose network connectivity (outside the hospital)?
* Was a new medical device installed?
* Was a medical device reconfigured? Was it reconfigured correctly?
* Other authorized events are causing excessive network traffic.
* Was an old process removed from the network?
* User error.

*IF* a cyber event is detected *AND* it cannot be explained, then we are compelled to perform integrity checks on EVERY server, workstation, router, network switch, firewall, controller, all printers and peripherals.

*WHEN* a cyber event is detected that may be a cyber-physical attack, a Cyber Event Ticket is created and the appropriate Hospital Incident Response Team is called upon to investigate.

# CYBERSECURITY CONTACTS

|  |  |
| --- | --- |
| Form Description | This form instructs employee who to notify when they discover a cyber-event has occurred or when they suspect an attack is underway. |
| Why it’s needed | Hospital employees need to react quickly to minimize hazards to patients. The form identifies who to contact and the telephone number. |
| Who fills it out | The Hospital Security Office, IT Office and Building Maintenance enter telephone numbers and post the information where hospital staff can see it. |
| How often updated | Form should always list current contact information. |

|  |  |
| --- | --- |
| Person discovering the cyber-event should call: | |
| Whom to Call | Telephone Number |
| IT Helpdesk |  |
| Building Operations Office |  |
| Security Office |  |
| IT Support Office |  |
| Whichever office is contacted first shall contact the other hospital offices. | |

# CYBERSECURITY BREACH REPORTING FORM – Page 1

|  |  |
| --- | --- |
| Form Description | This form is used to record a cyber-event that has occurred or when it is suspected an attack is underway. |
| Why it’s needed | The form requests information that may be valuable to defeat the cyber-attack and for preparing after-action report as well as to identify lessons learned to improve response in future. |
| Who fills it out | The hospital staff that is first contacted requests the information from the caller and distributes to other offices using both email and telephone messages while being sure other appropriate backup personnel and designated managers are contacted. |
| How often updated | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| The office alerted of the cyber-event will log: | |
| Name of the caller |  |
| Time of the call |  |
| Contact information about the caller |  |
| Caller physical location |  |
| The nature of the cyber-event |  |
| How was the cyber-event detected? |  |
| What equipment or persons were involved? |  |
| Location of equipment or persons involved |  |
| **Description of Breach** (select all that apply):  [ ]Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape)  [ ]Internal system breach  [ ]Insider wrongdoing  [ ]External system breach (e.g., hacking)  [ ]Active Medical Device Corrupted  [ ]Passive Medical Device Corrupted  [ ]Inadvertent disclosure  [ ]Other (specify): | |

# CYBERSECURITY BREACH REPORTING FORM – Page 2

|  |  |
| --- | --- |
| **The staff member could possibly add the following:** | |
| Is this event an Emergency? |  |
| Are active medical devices affected? |  |
| Has the Medical Staff been alerted? |  |
| What is the severity of the potential impact? |  |
| Were critical hospital building systems affected? |  |
| Name of equipment being targeted, along with operating system, IP address, and location. |  |
| IP address and any information about the origin of the attack. |  |

# INCIDENT RESPONSE TEAM STRATEGY MEETING FORM

|  |  |
| --- | --- |
| **Form Description** | This form is used to record how the Incident Response Team assesses the situation when a cyber-attack is underway. |
| **Why it’s needed** | The form requests information for preparing after-action report as well as to identify lessons learned to improve response in future. |
| **Who fills it out** | The Incident Response Team Leader. |
| **How often updated** | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| **Hospital Incident Response Team Initial Meeting/Discussion** | |
| Is the cyber event real or perceived? |  |
| Is the cyber event still in progress? |  |
| What equipment or system is threatened and how critical is it? |  |
| What is the impact on the hospital should the attack succeed? Minimal, serious, or critical? |  |
| Where is the equipment located physically and on the network? |  |
| Is the cyber event inside the trusted network? |  |
| Is the response urgent? |  |
| Can the cyber event be quickly contained? |  |
| Will the response alert the attacker and do we care? |  |
| What type of cyber event is this? | virus, worm, intrusion, abuse, damage |

# CYBER-EVENT DIAGNOSTICS TABLE

|  |  |
| --- | --- |
| Form Description | This form is used to record the observable events that led to discovery that a cyber-attack was underway. |
| Why it’s needed | The form requests information for preparing after-action report as well as to identify lessons learned to improve response in future. |
| Who fills it out | The Incident Response Team Leader. |
| How often updated | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| Check | Anomalous Behavior Observables |
|  | Unusually heavy hospital network traffic |
|  | Out of disk space or significantly reduced free disk space |
|  | Unusually high CPU usage |
|  | Creation of new user accounts |
|  | Attempted or actual use of administrator-level accounts |
|  | Locked-out accounts |
|  | Accounts in use when the hospital employee is not at work |
|  | Cleared log files |
|  | Full log files with an unusually large number of events |
|  | Antivirus or IDS alerts |
|  | Disabled antivirus software and other security controls |
|  | Unexpected patch changes |
|  | Active Medical Devices connecting to outside IP addresses |
|  | Requests for information about the network (social engineering attempts) |
|  | Unexpected changes in a medical device’s configuration settings |
|  | Unexpected system shutdowns |
|  | Stoppage or displayed error messages on a web, database, or application server |
|  | Unusually slow access to hosts on the hospital network |
|  | Filenames containing unusual characters or new or unexpected files and directories |
|  | Auditing configuration changes logged on the host records, disabling auditing function |
|  | A large number of bounced e-mails with suspicious content |
|  | Unusual deviation from typical hospital network traffic flows |
|  | Erratic hospital building equipment behavior, more than one active medical device exhibits the same anomalous behavior |
|  | Any apparent override of safety, backup, or failover systems |
|  | Equipment, servers, or hospital network traffic that has bursts of temporary high usage when the operational process itself is steady and predictable. |
|  | Unknown or unusual traffic from corporate network to hospital computer network |
|  | Unknown or unexpected firmware pulls or pushes |
|  | Loss of building utilities (electricity, water, gas, sewer equipment failure) |
|  | Large number of complaints from medical staff |
|  | Failure of multiple types of medical or building devices simultaneously |
|  | Very high energy usage |
|  | Obviously erroneous readings in medical device displays |

# Integrity Check Table

|  |  |
| --- | --- |
| Form Description | This form is used to record the action taken to verify the integrity of various pieces of equipment when a cyber-attack occurs. |
| Why it’s needed | The form provides information for recommended action to validate the integrity of the network and for preparing after-action report as well as to identify lessons learned to improve response in future. |
| Who fills it out | The Incident Response Team Leader. |
| How often updated | Form should be updated as new information is learned. |

|  |  |  |
| --- | --- | --- |
| Check | Device Integrity | Description |
|  | Computer Unresponsive | **BOOT** from Rescue CD, use tools to uncover problems. |
|  | Software Processes | **REVIEW** processes to identify malicious activity. Includes data base servers, control servers, HMIs, OPCs, master terminal units (MTUs), and engineering workstations. |
|  | Log Files | **REVIEW** database servers, HMIs, control server, engineering workstations, OPCs, MTUs and firewall log files for anomalies. |
|  | Registry | **IDENTIFY** changes and anomalies in the registry. |
|  | Rootkit | **CHECK** devices for a rootkit. |
|  | Network Communications | **VERIFY** network communications to the expected communications based on baseline. **VERIFY** data flow, and compare to baseline. |
|  | Unauthorized User Activity | **REVIEW** host log files for user account changes. |
|  | Firewalls | **DETERMINE** if configuration files, access control lists, operating system have been modified. **REVIEW** log file for anomalies or if log files have been modified. |
|  | Switches and Routers | **DETERMINE** if startup configuration, running configuration or operating system files have been modified. |
|  | Controllers | **VERIFY** the operating system, configuration files, and firmware against baseline. Includes PLCs, Intelligent electronic devices and remote terminal units. |
|  | Intrusion Detection System IDS Alerts – Inbound ICS Protocol | **DETERMINE** if IDS configuration files, rules, operating system, firmware, or log files have been modified. **DETERMINE** if the communications coming from the originating IP address should be communicating with the destination device. |
|  | Peripherals and Other Network Devices | **DETERMINE** if device has configuration files, operating system and whether they have been modified. |
| **☐** | Active Medical Devices | **DETERMINE** if medical device has configuration files, operating system and whether they have been modified. |

|  |  |
| --- | --- |
| Form Description | This form is used to record the action taken to determine the extent of damage to the building when a cyber-attack has taken place. |
| Why it’s needed | The form provides point of contact information and for preparing after-action report as well as to identify lessons learned to improve response in future. |
| Who fills it out | The Incident Response Team Leader. |
| How often updated | Form should be updated as new information is learned. |

# Hospital Building Inspection – Page 1

|  |  |
| --- | --- |
| Who Does the Inspection? | Facilities Engineers, Architects, Structural, Mechanical and Electrical Engineers, Security Officer, Safety Officer, City or County Building, Health and Fire Inspectors. |
| What Do They Inspect? | General property inspection and collection of records and if necessary, information needed to repair or replace damaged equipment. A **Rapid Inspection** is followed by a detailed **Engineering Inspection**. Engineers will inspect building columns, walls, ceilings, roof, masonry, windows and doors for obvious hazards. They will also inspect stairs and elevators for safety hazards. Stuck doors and sagging ceilings can be indicators of structural weakness. |
| Why Are They Doing the Inspection? | To identify damage in the building and reduce or permanently eliminate future risk to lives and property. Inspectors will take photographs and document the damage for reporting purposes and planning building repairs. |
| When Do They Do the Inspection? | Inspections are conducted immediately after the incident as soon as building is accessible and/or when allowed entry by local officials. |
| What is the Result of the Inspection? | Obtain the local permits, certificates of occupancy, and any other required documentation to demonstrate compliance with local building/zoning/life safety regulations. |
| What if the building does not pass inspection? | Develop a project plan and obtain necessary funding and approvals for building restoration and repairs. If the building is a complete loss, develop a plan to replace the building. |

# Hospital Building Inspection – Page 2

|  |  |
| --- | --- |
| Agency | Contact Information |
| City Building Department |  |
| Dept. of Public Works |  |
| Fire Department |  |
| Emergency Management |  |
| CERT |  |
| FEMA |  |
| Electric Utility Company |  |
| Natural Gas Utility Company |  |
| Water and Sewer Utility |  |

|  |  |
| --- | --- |
| Form Description | This form is used to record the action taken to determine the extent of damage to other systems when a cyber-attack has taken place. |
| Why it’s needed | The form provides information on the condition of various systems for preparing a response and after-action report as well as to identify lessons learned to improve response in future. |
| Who fills it out | The Incident Response Team Leader. |
| How often updated | Form should be updated as new information is learned. |

## Other Hospital Equipment to be Checked

|  |  |
| --- | --- |
| System | Description |
| Fire Detection System |  |
| Parking Garage Controls System |  |
| Traffic Barriers |  |
| Elevators |  |
| Fire Pumps |  |
| Smoke Evac System |  |
| Lighting Controls |  |
| Security Systems |  |
| Closed Circuit TV |  |
| Access Control System |  |
| Storm Drainage System |  |
| Incinerators |  |
| Fire Sprinkler System |  |
| Domestic Hot Water System |  |
| Cable TV System |  |
| Public Address System |  |
| Energy Recovery Systems |  |
| Solar Energy System |  |
| Medium Voltage Electrical Distribution System |  |
| Low Voltage Electrical Distribution System |  |
| Electric Power Monitoring System |  |
| Duress Alarm Systems |  |
| Sewerage Pump System |  |
| Wastewater Pump System |  |
| Storm Drainage Utilities |  |
| Sanitary Sewerage Utilities |  |
| Door Locking System |  |

# Cyber Event Ticket

|  |  |
| --- | --- |
| Form Description | This form is used to record the action taken for a cyber-event. |
| Why it’s needed | The form provides point of contact, description of the malfunction, action taken to mitigate damage. Useful for preparing after-action report as well as to identify lessons learned to improve response in future. |
| Who fills it out | The Incident Response Team member responding to the call. |
| How often updated | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| Cyber Event #: | Hospital Work Order #: |
| Work Order Type: | Customer Ref #: |
| Report Date: | Work Order Status: |
| Building: | Asset Worked On: |
| Additional Location Information: | |
| Customer Request: | |
| Conditions Found: | |
| Actions Taken: | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Status: |  | | Date: |  |
| Date: | Technician Name | Start Time | Stop Time | Regular Hours | OT Hours |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Part # | Description | | Quantity | Unit Cost | Total Cost |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
| Supply Rep Name | | Technician Name/ Date Received | | Supervisor Approval for High Value Items | |
|  | |  | |  | |
| Customer Signature & Date Completed | | | Customer Rating | | |
| x | | |  | | |
| Technician Signature & Date Completed | | | Customer Comment | | |
| x | | |  | | |
| QC Inspector Signature & Date Completed | | | QC Comment | | |
| x | | |  | | |

|  |  |
| --- | --- |
| Event Category. Event will be categorized into the highest applicable level of one of the following categories (Pick One): | |
| Event Category | Description |
| One | An immediate threat to patient life safety, hospital staff or the public |
| Two | An immediate threat to critical hospital buildings or utilities |
| Three | A threat to hospital computer systems |
| Four | A minor disruption of hospital services |

# Equipment or Service Failure Report

|  |  |
| --- | --- |
| Form Description | This form is used to describe the equipment that failed. |
| Why it’s needed | The form provides a description of the malfunction discovered and the extent of repairs. Useful for preparing after-action report as well as to identify lessons learned to improve response in future. |
| Who fills it out | The Incident Response Team member responding to the call. |
| How often updated | Form should be updated as new information is learned. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Building: |  | | Date: | | Report No.: | |  |
| Area affected and phenomenon or condition failure: | | | | Partial Failure | | Complete Failure | |
|  | | | | | | | |
| Mode of Discovery: | Alarm | Rounds/  Inspection | Abnormal Equip Operation | | Medical Staff Complaint | | Preventive Maintenance |
| Description of equipment or services that failed: | | | | | | | |
|  | | | | | | | |
| Emergency or temporary measures and containment actions: | | | | | | | |
|  | | | | | | | |
| Final or subsequent repairs: | | | | | | | |
|  | | | | | | | |
| Repaired by: | |  | | | | | |
| Defect: | Open | Closed | | | | | |
|  | | | | | | | |
| Remedial Action Required: | | | | | | | |
|  | Yes  No | | | | | | |
| Describe: | | | | | | | |

|  |  |
| --- | --- |
| Hospital personnel on duty at time of incident: | |
|  |  |
|  |  |
|  |  |

|  |
| --- |
| Findings and Conclusions: |
|  |
| Was this a cyber-attack? |

|  |
| --- |
| Explain: |

|  |
| --- |
| Is the area safe for patients, hospital employees or vendors? |
|  |
| Can equipment under examination function, and if so, at what percent of normal capacity? |
|  |
| What must be done to recover damaged equipment? |
|  |
| How long will it take to repair or replace the damaged equipment? |
|  |

Using the damage assessment, determine the estimated time to recover based on the following guidelines:

* **Level I - Minimal damage** to hospital facility and/or medical devices. Estimated time to complete repairs is less than 4 hours.
* **Level II - Moderate damage** to hospital facility and/or medical devices. Estimated time to complete repairs is between 4 hours and 2 business days.
* **Level III - Extensive damage** to hospital facility and/or medical devices. Estimated time to complete repairs is greater than 2 business days.

|  |  |
| --- | --- |
|  | Identify equipment or spare parts which are immediately salvageable or in need of repair. |
|  | Verbally notify the Hospital Administrator of survey results, assessment of damage, and rough estimate of time to recover. |
|  | Document findings from the survey and damage assessment. |
|  | Attend the recovery briefing to apprise Hospital Incident Recovery Team members of findings. |
|  | A log is prepared and maintained to record all salvageable equipment and its disposition and location. |

# Hospital Incident Response Team Member Listing

|  |  |
| --- | --- |
| Form Description | This form is used to identify individuals on the Incident Response Teams. |
| Why it’s needed | The form provides a comprehensive list of Team members, their contact info and when they were notified of the event. |
| Who fills it out | The Incident Response Team members provide info to Team Leader. |
| How often updated | Form should be updated as new information is learned. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Team Member Name | Cell Phone | Telephone | Time Called | E-mail |
| Management Team |  |  |  |  |
| Leader |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Facilities Team |  |  |  |  |
| Leader |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Tech Support Team |  |  |  |  |
| Leader |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Security Team |  |  |  |  |
| Leader |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

This list should be filled out and kept current.

# Repair Work Order Listing

|  |  |  |  |
| --- | --- | --- | --- |
| Priority | Task Number | Summary | Estimated Completion Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Recovery and Device Reintegration

|  |  |
| --- | --- |
| Form Description | This form is used to identify which Incident Response Team does what. |
| Why it’s needed | The form is a checklist listing the tasks needed to restore equipment, who performs the task, when they start the task and when the task is estimated to be complete. |
| Who fills it out | The Incident Response Team member provide info to Team Leader. |
| How often updated | Form should be updated as new information is learned. |

Effective recovery after a cyber-attack requires ensuring that new reintegration devices will not be re-infected. The only way to avoid this problem is to verify that each device on the network is clean of any cyber incident remnants. All devices in the network should be replaced or re-flashed with known, good firm/software to provide confidence that re-infection will not occur.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Task No. | Prior Task | Description | IRT Team | Estimated Start | Estimated Finish |
|  |  | **RESTART** undamaged equip – manual control | FAC |  |  |
|  |  | **PURCHASE** new hospital facility equipment | FAC |  |  |
|  |  | **INSTALL** new hospital facility equipment | FAC |  |  |
|  |  | **RUN** new equipment – manual mode | FAC |  |  |
|  |  | **RECEIVE** new network equipment | Tech |  |  |
|  |  | **INSTALL** software from vendor CD-ROMs | Tech |  |  |
|  |  | **INSTALL** new servers | Tech |  |  |
|  |  | **BOOT** the servers | Tech |  |  |
|  |  | **TEST** operating system | Tech |  |  |
|  |  | **TEST** network | Tech |  |  |
|  |  | **TEST** medical devices | Tech |  |  |
|  |  | **CONNECT** hospital facility equip to the BCS | MGMT/FAC/Tech |  |  |
|  |  | **TEST** BCS with hospital facility equipment | MGMT/FAC/Tech |  |  |
|  |  | **ADVISE** Hospital Administration | MGMT |  |  |
|  |  | **REASSESS** the situation | MGMT |  |  |
|  |  | **SCHEDULE** move dates for patient return | MGMT/FAC/Tech |  |  |
|  |  | **ESTABLISH** new building operating schedule | MGMT/FAC/Tech |  |  |
|  |  | **MOVE** patients back to hospital | MGMT |  |  |
|  |  | **RESUME** normal hospital operations | MGMT/FAC/Tech |  |  |
|  |  | **MONITOR** help desk for medical staff concerns | MGMT/FAC/Tech |  |  |
|  |  | **PREPARE** media statements | MGMT/SEC |  |  |
|  |  | **PREPARE** after-action report | MGMT/FAC/Tech |  |  |
|  |  | **UPDATE** Recovery Procedure w/Lessons Learned | MGMT/FAC/Tech |  |  |

# Building Controls System Recovery and Reintegration

|  |  |
| --- | --- |
| Form Description | This form lists recovery and reintegration tasks. |
| Why it’s needed | The form is a checklist listing the tasks needed to restore equipment and the order in which they are to be completed. |
| Who fills it out | The Incident Response Team member provide info to Team Leader. |
| How often updated | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| The following Recovery and Reintegration checklists apply to all devices on the BCS network: | |
| Servers | |
| Workstations | |
| Routers/Switches/Modems/Printers | |
| Remote Terminal Units (RTU)/MTU/PLC | |
| IEDs; Controllers, Breakers, Switches, Re-closers, Regulators | |
| Human-Machine Interface (HMI) | |
| Firewalls | |
| Media Converters (Serial to Fiber, Serial to Ethernet) | |
|  | |
| **BCS Recovery** | |
|  | **DOCUMENT** steps taken during recovery procedures for forensic analysis of the cyber incident and possible use as evidence later on. |
|  | **MAINTAIN** primary power (if possible) to the BCS device until an image can be saved of the onboard memory. |
|  | **SAVE** an image of any hard drive(s) and volatile memory (if possible) for forensic analysis. This may require a reboot. **CAPTURE** volatile memory first, and then image the drive. |
|  | **REMOVE and REPLACE** the affected BCS device. |
|  | **DO NOT** **REIMAGE** any devices. Reimaging the affected device drive(s) will destroy forensic evidence of the cyber incident. |
|  | **VERIFY** the latest operating system, software, and firmware patches are installed on the device. **INSTALL** updates prior to reintegration in the BCS. |
|  | **UPDATE** passwords on all BCS devices (including seldom used obscure modules). |
|  | **UPDATE** the antivirus software and intrusion detection software and **RUN** a full system scan. |
| **BCS Reintegration** | |
|  | **DO NOT** **RECONNECT** the device to other devices in the network until each device in the affected network layer or affected sub-system has been recovered per these procedures. |
|  | **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. **CONSULT** the cyber incident records to confirm that *Recovery* has been performed on these devices prior to reintegration on the BCS network. |
|  | When each device in the layer or sub-system has been properly recovered and documented, **RECONNECT** all of the devices. |
|  | **DO NOT** **RECONNECT** to the enterprise network. |
|  | **VERIFY** that the forensics specialists have eliminated cyber incident artifacts using detection tools (IDS, Log Review, NMap, Netstat, Wireshark, etc) and documented the results. |
|  | **MONITOR** the BCS for anomalous BEHAVIOR. |
|  | If anomalous behavior is still evident, **REPEAT** the detection procedures and/or mitigation procedures as necessary. |
|  | When the layer or sub-system is operating without evidence of the cyber incident, and the Recovery Procedures Coordinator gives approval, **RECONNECT** the isolated layer or sub-system to the BCS. |
|  | **MONITOR** the system for anomalous behavior. |
|  | If anomalous behavior is still evident, **REPEAT** the detection procedures and/or mitigation procedures as necessary. |
|  | **SUBMIT** all records of recovery actions to the Recovery Procedures Coordinator. |
|  | **RETURN** to Routine Monitoring of the network. |

**CUSTOMIZE** form for your specific hospital and verify the normal operating conditions when the recovery procedures are prepared.

## Building Controls System Field Test

All point-to-point testing of end field devices through proper input/output to graphic and operator interface shall be completed and approved.

All field calibration shall be completed and approved.

Detailed functional tests shall verify that the system adheres to the Sequence of Operation.

All alarm limits shall be completed and approved.

All schedule start/stops and system setpoints shall be entered, operating and approved.

**General:** Adjust, calibrate, measure, program, configure, set the time schedules, and ensure that the systems function as specified in the Sequence of Operations.

**Systems Check:** An item by item check shall be performed for each HVAC system.

* **Step 1** - **System Inspection:** With the system in unoccupied mode and with fan hand-off-auto switches in the OFF position, it shall be verified that power and main air are available where required and that all output devices are in their failsafe and normal positions. Each local display panel and each M&C Client shall be inspected to verify that all displays indicate shutdown conditions.
* **Step 2** - **Calibration Accuracy Check:** A two-point accuracy check of the calibration of each HVAC control system sensing element and transmitter shall be performed by comparing the value from the test instrument to the corresponding SNVT. Digital indicating test instruments shall be used, such as digital thermometers, motor-driven psychrometers, and tachometers. The test instruments shall be at least twice as accurate as the specified sensor accuracy. The calibration of the test instruments shall be traceable to National Institute of Standards and Technology standards. The first check point shall be with the HVAC system in unoccupied mode with fan hand-off-auto switches in the OFF position, and the second check point shall be with the HVAC system in an operational condition. Calibration checks shall verify that the sensing element-to-DDC system readout accuracies at two points are within the specified product accuracy tolerances. If not, the device shall be recalibrated or replaced and the calibration check repeated.
* **Step 3** - **Actuator Range Check:** With the system running, a signal shall be applied to each actuator through the DDC Hardware controller. Proper operation of the actuators and positioners for all actuated devices shall be verified and the signal levels shall be recorded for the extreme positions of each device. The signal shall be varied over its full range, and it shall be verified that the actuators travel from zero stroke to full stroke within the signal range. Where applicable, it shall be verified that all sequenced actuators move from zero stroke to full stroke in the proper direction, and move the connected device in the proper direction from one extreme position to the other.

## Operational Security Log

|  |  |
| --- | --- |
| Form Description | This form is used to identify physical security safeguards that were implemented by Team members. |
| Why it’s needed | The form lists the equipment that needs to be safeguarded, when the equipment was secured and how it was secured. This will support the chain of custody for evidence later on as well as for the after action report. |
| Who fills it out | The Incident Response Team member provide info to Team Leader. |
| How often updated | Form should be updated as new information is learned. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date:**  **Time** | **Asset** | **Operator:**  **IP Address** | **Description** | **Action Taken** | **Results** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Medical Network Recovery and Device Reintegration

|  |  |
| --- | --- |
| Form Description | This form lists recovery and reintegration tasks for medical grade network and medical devices. |
| Why it’s needed | The form is a checklist listing the tasks needed to restore equipment and the order in which they are to be completed. |
| Who fills it out | The Incident Response Team member provide info to Team Leader. |
| How often updated | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| The following Recovery and Reintegration checklists apply to all devices on the networks: | |
| Servers | |
| Workstations | |
| Routers/Switches/Modems/Printers | |
| Remote Terminal Units (RTU)/MTU/PLC | |
| IEDs; Controllers, Breakers, Switches, Re-closers, Regulators | |
| Human-Machine Interface (HMI) | |
| Firewalls | |
| Media Converters (Serial to Fiber, Serial to Ethernet) | |
| Medical Devices | |
| **Network Recovery** | |
|  | **DOCUMENT** steps taken during recovery procedures for forensic analysis of the cyber incident and possible use as evidence later on. |
|  | **MAINTAIN** primary power (if possible) to the medical device until an image can be saved of the onboard memory. |
|  | **SAVE** an image of any hard drive(s) and volatile memory (if possible) for forensic analysis. This may require a reboot. **CAPTURE** volatile memory first, and then image the drive. |
|  | **REMOVE** and **REPLACE** the affected device. |
|  | **DO NOT** **REIMAGE** any medical devices. Reimaging the affected device drive(s) will destroy forensic evidence of the cyber incident. |
|  | **VERIFY** the latest operating system, software, and firmware patches are installed on the device. **INSTALL** updates prior to reintegration in the network. |
|  | **UPDATE** passwords on all devices (including seldom used obscure modules). |
|  | **UPDATE** the antivirus software and intrusion detection software and **RUN** a full system scan. |
| **Device Reintegration** | |
|  | **DO NOT** **RECONNECT** the device to other devices in the network until each device in the affected network layer or affected sub-system has been recovered per these procedures. |
|  | **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. **CONSULT** the cyber incident records to confirm that *Recovery* has been performed on these devices prior to reintegration on the hospital network. |
|  | When each device in the layer or sub-system has been properly recovered and documented, **RECONNECT** all of the medical devices. |
|  | **DO NOT** **RECONNECT** to the enterprise network. |
|  | **VERIFY** that the forensics specialists have eliminated cyber incident artifacts using detection tools (IDS, Log Review, NMap, Netstat, Wireshark, etc) and documented the results. |
|  | **MONITOR** the network for anomalous **BEHAVIOR**. |
|  | If anomalous behavior is still evident, **REPEAT** the detection procedures and/or mitigation procedures as necessary. |
|  | When the layer or sub-system is operating without evidence of the cyber incident, and the Recovery Procedures Coordinator gives approval, **RECONNECT** the isolated layer or sub-system to the network. |
|  | **MONITOR** the system for anomalous behavior. |
|  | If anomalous behavior is still evident, **REPEAT** the detection procedures and/or mitigation procedures as necessary. |
|  | **SUBMIT** all records of recovery actions to the Hospital Recovery Procedures Coordinator. |
|  | **RETURN** to Routine Monitoring of the network. |

**CUSTOMIZE** form for your specific hospital and verify the normal operating conditions when the recovery procedures are prepared.

## Hospital Data Network Information

|  |  |
| --- | --- |
| Form Description | This form lists vital information for critical network equipment. |
| Why it’s needed | The form is a checklist listing the information needed to restore equipment after a cyber-attack. |
| Who fills it out | The Incident Response Team members. |
| How often updated | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| Date Updated |  |
| Unique Application ID |  |
| Application Name |  |
| Owner (e.g., Department, etc.) |  |
| Custodian (e.g., departmental IT staff, vendor) |  |
| Description |  |
| User Base/Scope |  |
| Business Function |  |
| Data Classification |  |
| Criticality |  |
| Date of Last Business Impact Analysis (BIA) |  |
| Operating System |  |
| Asset Tag |  |
| Serial Number |  |
| Licensing Information |  |
| Vendor (or, internally developed) |  |
| Maintenance Contract Expires |  |
| Maintenance Contact |  |
| Current Instances (e.g., production and test, test only, production only) |  |
| Program Language (s) |  |
| Internet Accessible |  |
| Requires own server |  |
| Desktop Data Storage (e.g., what files/configuration are required if app allows or requires storage of data on workstations) |  |
| External File Requirements |  |
| Domain Information |  |
| Service Account (s) |  |
| Storage Requirements |  |
| Seats/Units |  |
| Load Balancing |  |
| License Requirements |  |
| Protocol Requirements |  |
| Port Requirements |  |
| Network Requirements |  |
| IP Address/Range |  |
| Minimum Client Requirements |  |
| Encryption Requirements |  |
| Third Party Requirements (e.g., applications or software required) |  |
| Code Libraries |  |
| Known Bottlenecks |  |
| Batch Processing Details (e.g., scheduled tasks, duration, subtasks, etc.) |  |
| Backup Software |  |
| Backup Type |  |
| Backup Frequency/Schedule |  |
| Media |  |
| Offsite Storage Location |  |
| Generations Offsite |  |
| Source Code Backed Up? |  |
| Additional Details |  |
| Maintenance Window Details |  |
| Vendor /Internal contact information |  |
| Recovery Point Objective (RPO) |  |
| Recovery Time Objective (RTO) |  |
| Priority |  |
| Additional Details |  |
| Supporting Documentation Location |  |
| Additional Details |  |
| Application is dependent on the following hardware resources: |  |
| Other Processes dependent on this application: |  |
| Applications/services etc. dependent on this resource: |  |
| Applications/services etc. this resource is dependent on: |  |

This list should be filled out and kept current.

## Building Controls System Network Information

|  |  |
| --- | --- |
| Form Description | This form lists vital information for critical BCS network equipment. |
| Why it’s needed | The form is a checklist listing the information needed to restore equipment after a cyber-attack. |
| Who fills it out | The Incident Response Team members. |
| How often updated | Form should be updated as new information is learned. |

|  |  |
| --- | --- |
| Date Updated |  |
| Unique Application ID |  |
| Application Name |  |
| Owner (e.g., Department, etc.) |  |
| Custodian (e.g., departmental IT staff, vendor) |  |
| Description |  |
| User Base/Scope |  |
| Business Function |  |
| Data Classification |  |
| Criticality |  |
| Date of Last Business Impact Analysis (BIA) |  |
| Operating System |  |
| Asset Tag |  |
| Serial Number |  |
| Licensing Information |  |
| Vendor (or, internally developed) |  |
| Maintenance Contract Expires |  |
| Maintenance Contact |  |
| Current Instances (e.g., production and test, test only, production only) |  |
| Program Language (s) |  |
| Internet Accessible |  |
| Requires own server |  |
| Desktop Data Storage (e.g., what files/configuration are required if app allows or requires storage of data on workstations) |  |
| External File Requirements |  |
| Domain Information |  |
| Service Account (s) |  |
| Storage Requirements |  |
| Seats/Units |  |
| Load Balancing |  |
| License Requirements |  |
| Protocol Requirements |  |
| Port Requirements |  |
| Network Requirements |  |
| IP Address/Range |  |
| Minimum Client Requirements |  |
| Encryption Requirements |  |
| Third Party Requirements (e.g., applications or software required) |  |
| Code Libraries |  |
| Known Bottlenecks |  |
| Batch Processing Details (e.g., scheduled tasks, duration, subtasks, etc.) |  |
| Backup Software |  |
| Backup Type |  |
| Backup Frequency/Schedule |  |
| Media |  |
| Offsite Storage Location |  |
| Generations Offsite |  |
| Source Code Backed Up? |  |
| Additional Details |  |
| Maintenance Window Details |  |
| Vendor /Internal contact information |  |
| Recovery Point Objective (RPO) |  |
| Recovery Time Objective (RTO) |  |
| Priority |  |
| Additional Details |  |
| Supporting Documentation Location |  |
| Additional Details |  |
| Application is dependent on the following hardware resources: |  |
| Other Processes dependent on this application: |  |
| Applications/services etc. dependent on this resource: |  |
| Applications/services etc. this resource is dependent on: |  |

This list should be filled out and kept current.

# Medical Device and Equipment Vendor Contact List

|  |  |
| --- | --- |
| Form Description | This form is used to identify equipment representatives. |
| Why it’s needed | The form provides a comprehensive list of manufacturer’s field maintenance personnel, their contact info so they can be notified of the event quickly. |
| Who fills it out | The Incident Response Team members. |
| How often updated | Form should be updated as new information is learned. |

This is a listing of all vendors and contractors that currently provide support or will provide support in a post-disaster environment. Additionally, any Service Level Agreements (SLAs) that have been executed and all subsequent modifications should be attached.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vendor Contact List | | | | |
| Vendor | Equipment | Contact Name: | Telephone | Email |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## List of Authorized Maintenance Laptop Computers

|  |  |
| --- | --- |
| Form Description | This form is used to identify hospital laptop computers that are approved for use on the network. |
| Why it’s needed | The form provides a comprehensive list of approved equipment including the date of the most recent virus scan. |
| Who fills it out | The Incident Response Team member provide info to Team Leader. |
| How often updated | Form should be updated as new information is learned. |

The Authorized Maintenance Laptop List may be unique to each building and should be readily available to the IRT. The list includes the date of the last virus scan for each. Authorized maintenance laptops MUST be stored in a secure location and only issued to vendors on site for use on site. When needed for more than one day, laptops shall be collected at the end of each day and locked away. Laptop shall be scanned for virus and malware prior to connection to the BCS every time. After use, vendor software shall be wiped and drive scanned prior to returning to storage.

|  |  |
| --- | --- |
| Authorized Maintenance Laptop List | |
| Date of Last Virus Scan | Laptop Number |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Vulnerability Assessments History

|  |  |
| --- | --- |
| Form Description | This form identifies when the network was last scanned and the name of the company that performed the scan. |
| Why it’s needed | The form includes brief recommendations made by the company that performed the scan. |
| Who fills it out | The Incident Response Team Leader. |
| How often updated | Form should be updated as new information is learned. |

## Types of Internal and External Vulnerability Tests

**White-Box Test Team**

Test team has complete access to the hospital network including network diagrams, hardware, operating system and application details. Knowledge of hospital network allows targeting specific building equipment, applications and active medical devices.

**Grey-Box Test Team**

Test team simulates attack by a disgruntled employee. Test team has user-level privileges and access permitted to the hospital network with certain security policies relaxed.

**Black-Box Test Team**

Test team has no prior knowledge of hospital network (except possibly a website URL or IP address). Test team attempts to break into the hospital network remotely.

|  |  |  |  |
| --- | --- | --- | --- |
| Scan Date | Testing Team & Type | Company | Recommendations |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vulnerability Test Types**

1. **External Vulnerability Scan** - Identify network-facing vulnerabilities (Monthly).
2. **Internal Vulnerability Scan** - Identify network-facing vulnerabilities (Quarterly).
3. **External Vulnerability Assessment** - Identify configuration and architecture vulnerabilities (Annual).
4. **Internal Vulnerability Assessment** - Identify network, client, configuration and physical vulnerabilities (Annual).
5. **Penetration Test** - Exploit any vulnerability to obtain access to building controls (Annual).

**Vulnerabilities Notifications Reports**

|  |  |
| --- | --- |
| Form Description | The following forms list the vulnerabilities that were announced for equipment the hospital maintains, indicates when the vulnerability was announced, the impact of the vulnerability if not fixed and when the patch was installed. |
| Why it’s needed | The forms include a brief description of the vulnerability and the system affected. |
| Who fills it out | The Incident Response Team Leader. |
| How often updated | Form should be updated as new information is learned. |

# Hospital Data Network Vulnerabilities Notifications Report

Below is a list of announced system vulnerabilities for the Hospital Data Network.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Announced Hospital Network Vulnerabilities** | | | | | |
| Bulletin ID. or Name | Description | System Affected | Release Date | Resolved | Impact |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Hospital Data Network Software Management Report

Below is a list of installed and missing Service Packs on the Hospital Data Network.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Installed and Missing Service Packs | | | | | | | | |
| Bulletin ID. or Name | Description | System Affected | Release Date | Severity | Lab Test Date | Patch Date | Complete Pending | Name of Tester |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

# Building Controls System Network Vulnerabilities Notifications Report

Below is a list of announced system vulnerabilities for the Building Controls System.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Announced Hospital Network Vulnerabilities | | | | | |
| Bulletin ID. or Name | Description | System Affected | Release Date | Resolved | Impact |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Building Controls System Network Software Management Report

Below is a list of installed and missing Service Packs on the Building Controls System.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Installed and Missing Service Packs | | | | | | | | |
| Bulletin ID. or Name | Description | System Affected | Release Date | Severity | Lab Test Date | Patch Date | Complete Pending | Name of Tester |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Medical Device Data System Vulnerabilities Notifications Report**

Below is a list of announced system vulnerabilities for the Medical Device Data System.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Announced Hospital Network Vulnerabilities | | | | | |
| Bulletin ID. or Name | Description | System Affected | Release Date | Resolved | Impact |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Medical Device Data System Software Management Report

|  |  |
| --- | --- |
| Form Description | The form lists the software updates that were announced for equipment the hospital maintains. |
| Why it’s needed | The form indicates when the software patch was available for each system, the impact of the vulnerability if not fixed, and when the patch was installed and tested and who conducted the test. |
| Who fills it out | The Incident Response Team Leader. |
| How often updated | Form should be updated as new information is learned. |

Below is a list of installed and missing Service Packs on the Medical Grade Network.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Installed and Missing Service Packs | | | | | | | | |
| Bulletin ID. or Name | Description | System Affected | Release Date | Severity | Lab Test Date | Patch Date | Complete Pending | Name of Tester |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |