Artifact D: Sample Roles for Breach Response

CIRT Roles and Responsibilities

Roles and Responsibilities

Within this section, the roles and responsibilities for the CIO/DCIO, Critical Incident Response/Recovery Sub-Team (CIRT), CIC, and Supporting Groups are defined. In addition, this section addresses the various IT Services functional areas within the University and their CIRT responsibilities.

The University has a pool of CICs. Should the initial CIC be unavailable or unavailable during the entire incident, then the CNOC or Support Desk should call the next CIC within 10 minutes.

- Ideally, the CICs should be matched to the type of critical incident occurring at the University.
- CICs should understand they may be asked to run an incident outside of their functional area.
- If the CIC is initially unavailable, an alternate will assume the CIC role in his/her stead.

Chief Information Officer / Deputy Chief Information Officer

This position will report directly to the University's President and Board of Trustee. This role will either involve or inform as the needs of the incident dictate. Communication of information during an incident will follow this flow to eliminate confusion and misinformation between groups.

The CIO/DCIO is responsible for executing or delegating the following:

- Setting priorities
- Notifying the University President and/or Board of Trustees of an incident declaration
- Communicating status of critical incident to the PEC
- Participating with CIC in forensic investigation decisions
- Designating the DCIO or an alternate to cover the responsibilities of the CIO role
- Notifying University Communications as appropriate for internal and external communication
- Owning of the CIC's incident work plan(s)
- Defining and issuing 'gag' orders within IT Services for particularly sensitive issues; the default guideline for communicating about a critical incident is on a need to know basis
- Notifying Human Resources as appropriate
- Notifying Legal as appropriate
- Notifying Campus Security as appropriate
- Chairing the Post Mortem – Closeout Phase

Critical Incident Coordinator (CIC)

This position will update the CIO/DCIO on a regular basis during a critical incident. The CIC will obtain technical expertise based on the incident declared.

The CIC is responsible for the following:

- Managing incident resources
- Determining if an incident is a Critical Incident and declaring it to be so.
- Maintaining communications between CIRT and the CIO/DCIO
- Reminding staff that communication is on a need to know basis or if the CIO has defined a 'gag order' informing team members and the CNOC of the nature of the 'gag'.
- Communicating to the CNOC and the IT Services Leadership Team that a critical incident has been declared and a CIRT has been formed
- Activating the CIRT and notifying the team of meeting locations and call-in telephone numbers
- Beginning a case file for the incident. Use to ensure information is properly collected and documented
- Developing containment procedures
- Establishing a Post Mortem Team to determine the root cause and root effect of the incident

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)

- Working closely with the CIO/DCIO and University Counsel during forensic investigations
- Managing the incident work plan(s) and task assignments
- Raising dependency issues as they arise
- Designating an alternate CIC to cover the responsibilities that span more than 12 hours
- Coordinating hand-off meetings between shifts, and developing work plans that address tasks completed and outstanding
- Certifying that all systems are returned to operational quality with the cause rectified
- The secure destruction/retention of all materials at the end of an incident
- Identifying external personnel/resources as needed
- Recommending to the CIO/DCIO, if warranted, that the critical incident be upgraded to a disaster

Resource Coordinator (CNOC)

The Resource Coordinator must maintain a current list of all contact information for the CIRT. The CNOC will play this role for critical incidents.

The Resource Coordinator is responsible for the following:

- Establishing the "war room" during a computer incident
- Providing appropriate networks, computers, phones, and faxes
- Designating a scribe to document CIRT activities and follow the work plan established by the CIC.
- Establishing food provisions and lodging

CIRT Response Team

During an incident the CIC will assemble a team. Members will vary depending on the skill sets required to assist during an incident. Teams will vary in size depending on the need. This team will remain active until the incident is closed. The members will include staff from the IT Services Division as described later in this document. This team will be responsible for both response and recovery.

Response. The response duties of the team are to conduct triage of the incident, assist in containment of the incident, collect evidence for the post mortem report and if requested, conduct or assist in a forensic investigation.

- Assisting in the collection of evidence during an incident investigation
- Making recommendations to the CIC on remedial action on affected systems
- The Response Team may be called up 24 hours a day, 7 days a week, 365 days a year during a critical incident

Recovery. The response aspects of the team are centered around damage assessment, return to normal operations, rebuilding serves and systems, etc.

- Determining whether affected systems can be restored from backup tapes, or must be reinstalled
- Scrubbing all data before making it ready for reinstall
- Determining what data is lost and cannot be recovered or restored
- Reloading data on affected systems
- Restoring normal operations

CIRT Post Mortem Team

The Post Mortem Team is assembled by the CIC, chaired by the CIO or the DCIO. This team is part of the Reactive Services "Maintenance". Their responsibilities are:

- Sending final incident reports to parties with a need-to-know
- Discussing procedural changes and updates
- Discussing configuration issues
- Deciding whether to conduct an investigation to determine what the root cause and root effects of the incident
- Discussing any task that were not completed

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)

- Deciding whether it is necessary to determining the Total Cost of Incident (TCI)
- Recommending updates to policies, procedures, standards and the Critical Incident Response Plan as necessary

Support Desk

- Initiates communications for critical incidents to the CIC during business hours.
- Provides liaison with the user community
- Provides liaison with the CNOC
- Provides informational announcement for serious incidents per the direction of the CIC or CIO/DCIO
- Assesses an incident's impact to the desktop computer environment
- Provides assistance with viruses, Trojan horses, and worms
- Collects, stores, and assists in desktop system audit data analysis as necessary
- Coordinates change management in the desktop environment
- Coordinates change testing for the desktop computer environment
- Coordinates, implements, maintains and certifies all Microsoft operating systems changes on desktop and server systems
- Certifies changes to the desktop environment
- Implements desktop changes

Computing & Network Operations Centers (CNOC)

- Provides the critical phones numbers for X University President and Board of Trustees manila folder. The folder is labeled "Contact Phones. Mgt: Pres Exec Council: Board of Trustee"
- Holds the call-out list for University resources. This list resides at the following URL: www.unitsmuohio.edu/mcs/techserv/noc/nocstaffonly/dreamweavernxfiles/phonelist.htm
- Initiates communications to the CIC as problems are detected or reported
- Responsible for coordination with emergency change management as directed by the CIC
- Monitoring of Intrusion Detection and/or Intrusion Prevention Systems
- Monitoring the Network using OpenView
- Assess alerts from the IDS/IPS
- Alerts the Support Desk to any incident for escalation
- Liaison with Red Siren

Security Office

- Creates security policies and procedures
- Create and maintain university security awareness
- Manage perimeter controls
- Oversight of Managed Security Services
- Oversee separation of duties for financial systems technical management
- System Hardware and software vulnerability analysis
- Create multiple platform technical and admin incident management procedures
- Perform system risk assessments
- Manage network user access. Disable and enable end-user accounts if required

Critical Incident Response Steering Committee *(proposed)*

- Appoint the Critical Incident Response Working Committee
- Receive requests for clarification and assistance from the Critical Incident Response Working Committee and advise them in their work
- Approve changes to the CIRP

Critical Incident Response Working Committee *(proposed)*

- Meet at least quarterly to update the CIRP
- Conduct training at least annually
- Receive recommendations from Post Mortem teams for improvements to CIRP
- Ongoing testing and evaluation of the CIRP operation

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)

Campus Safety and Security

- Assist in interviews when requested
- Assist human resources during policy violations
- Coordinate with external law enforcement as required
- Liaison to Federal Bureau of Investigations (FBI) as requested by University Counsel

Disaster Recovery Team *(not part of Critical Incident Response)*

- Manages the development and maintenance of the Disaster Recovery Plan
- Receive declaration of disaster that would upgrade a critical incident to a disaster
- Liaison with X University's recovery sites
- Interfaces with the CIO/DCIO and/or the CIC to ensure proper integration and coordination between the CIRP and other crisis management plans, as required by event circumstances (Disaster Recovery Plan, Hurricane Preparedness Plan)

University Counsel

- Provides guidance to the CIO regarding legal and regulatory aspects of the incident and its public disclosure
- Advises Human Resources regarding investigations involving employees
- Advises the CIO/DCIO and/or CIC regarding decision to simply protect its operations or to pursue civil or criminal actions
- Consults with the CIO/DCIO and/or CIC regarding involvement with law enforcement
- Advises the CIO/DCIO and/or CIC regarding involvement with regulatory agencies
- Reviews communications drafted by University Communications as required
- Liaison to external counsel

Human Resources

- Advises CIO/DCIO and/or CIC on personnel matters
- Initiates employee related investigations along with University Counsel
- Participates in investigation interviews and furnishes legally permissible personal information as necessary
- Alerts the CIRT of any unusual employee behavior patterns during a critical incident or investigation
- Manages internal rumors and fields internal questions from the employee base that are not associated with an incident
- Coordinates internal employee communications along with University Counsel, as necessary

University Communications

- Provides external communications in consultation with University Counsel
- Responds to all external media inquiries
- Liaison to external public relation firms
- Ensure internal communications are consistent with external communications

Operations and Telecommunications

- Establishes new lines and communications bridges as directed by the CIC
- Provides necessary communication lines for the CIRT War Room
- Assesses an incident's routing and transmission impact
- Provides log data to the CIRT as required
- Provides assistance to the CIRT related to modems
- Provides assistance investigating PBX accounts and permissions
- Liaison with the following: Anixter, Sprint North Supply, Accu-tech – Supply Chain, Magnum Cable, Westco, Famous Telephone, NEC Integrated Business Solutions (Labor contract with them), Cincinnati Bell

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.

Artifact D: Sample Roles for Breach Response (Cont.)

Technical Support

- Coordinates change management and testing for Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Coordinates, implements, maintains and certifies the Operating System Environment for all Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux operation systems.
- Assesses an incident's impact to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Certifies and implements changes to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment.
- Coordinates and implements patches to the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment
- Develops, maintains and implements hardening procedures for the Windows, Mac, Unix, AIX, Solaris, HPUX, Netware, and Linux server environment
- Responsible for the entire electronic mail system utilized by X University.
  - Coordinates changes to the electronic Mail environment
  - Implements changes to messaging systems
  - Assesses impact of email or messaging based malware (malicious code)
- Performs backup procedures on the server environment
- Liaison with IBM, Solaris, DNS-1, and SendMail
- Responsible for SAN administration

Communication and Networking

- Collects, stores, and assists in system audit data analysis as necessary for the routers and firewalls
- Coordinates, implements, maintains and certifies all routing changes and OS changes to network devices.
- Provides Firewall Services
  - Implements changes to the firewall rule sets to assist in incident containment as necessary
  - Provides rule sets to the CIRT as required
  - Provides log data to the CIRT as required
- Assesses an incident's impact to Wide Area Network and/or Local Area Network.
- Assists in identifying the impact to the perimeter and Internet facing environments.
- Assists in identifying the impact to X University's wireless network
- Plans, maintains and audits the network infrastructure

CSS

- Assist in evaluation of business continuity and disaster recovery solutions
- Plans, maintains and audits the network infrastructure

Information System and Services / Student Systems and Business Systems

- Responsible for the Banner system and applications
- Conduct software support for the Banner system and applications
- Implements changes to the Banner system and applications

Database Administration

- Rebuild and implement installation for the databases
- Builds and configures the databases
- Provides backup and recovery services for the databases
- Overall security for the databases

Network Applications Group

- Responsible for Blackboard Course Info, MyX, WAS, Account Generation

University Critical Incident Response Plan, https://net.educause.edu/Elements/Attachments/security/9320/MUOhio_CIR_Plan.pdf.