Laying the Groundwork for Response

The last thing a technology leader needs to do during a data emergency is quibble over wording or worry about the chain of command. An effective plan provides clear, unequivocal definitions of a data breach, and staff members responsible for identification and response.

These frames for critical definitions and decision ownership are illustrative, combined from the existing plans of several institutions; the most effective policies will reflect campus-specific culture and policies.

Artifact A: **The University of Iowa's** Incident Response Team's Workflow (p. 14) provides a visualization of incident triage.

Developing a Consistent Workflow to Triage Incidents

Does the Breach Affect a Critical System?

- *Hierarchy of Priorities:*
  - Human Life and Safety
  - Sensitive and Regulated Information*
  - Critical Networks and Systems
  - Business Continuity
  - Internal Customer Service

Who Owns Decisions During the Breach?

- *Security Officer*
  - Detect and Report Incident
- *Chief and Deputy Information Officer*
  - Approve Incident Category
  - Manage Internal Communication
- *Incident Response Leader*
  - Build Incident Response Team

Maintain a pool of potential incident response leaders that will be ready to lead breach operations when necessary; leaders will most likely come from the central IT office, but knowledge and operational ability trump department.

Response leaders need to be empowered to make spending and notification decisions, and will range in seniority appropriate to their incident.

Asking leaders to collect response metrics (e.g., mean time to fix problem) will help technology leaders measure the effectiveness of procedures against different breach types, and improve future response.

Incident Leader Coordinates, Measures Response

Responsibilities of the Incident Response Leader

Manage Internal Communication

- Define incident priority level and notify CIO if necessary
- Update key staff (e.g., CIO, General Counsel) on breach during investigation

Staff Response Team

- Recruit technical staff members with experience in compromised data
- As necessary, involve escalating group of key participants

Ensure Data Collection

- With technical team members, collect forensic evidence and KPI's
- Compile report on data breach and response for future security preparation

Incident Response is a 'Drop Everything' Priority

Make sure that response leaders have the authority to clear all other team responsibilities during response.

* At many institutions, this will include licensed research and other high-value targets.