Organizing Staff and Resources

When a breach occurs, quick action can staunch losses and expedite the mitigation process. Make sure that response leaders know and are authorized to carry out the actions that will mobilize response, limit damage, and collect necessary data on the breach.

Artifacts B-C: **Indiana University** templates for breach reporting and response (p. 15-16).

Know the Necessary Immediate Steps

Mobilize Response

- *Limit Damage:*
  - – Limit and secure access to compromised systems
  - – If necessary, shut down affected machines and networks until forensic support arrives
- *Alert Team:*
  - – Activate response leaders, who will be responsible for pulling in support personnel
  - – Alert external response component groups (e.g., forensic data specialists)

Collect Information

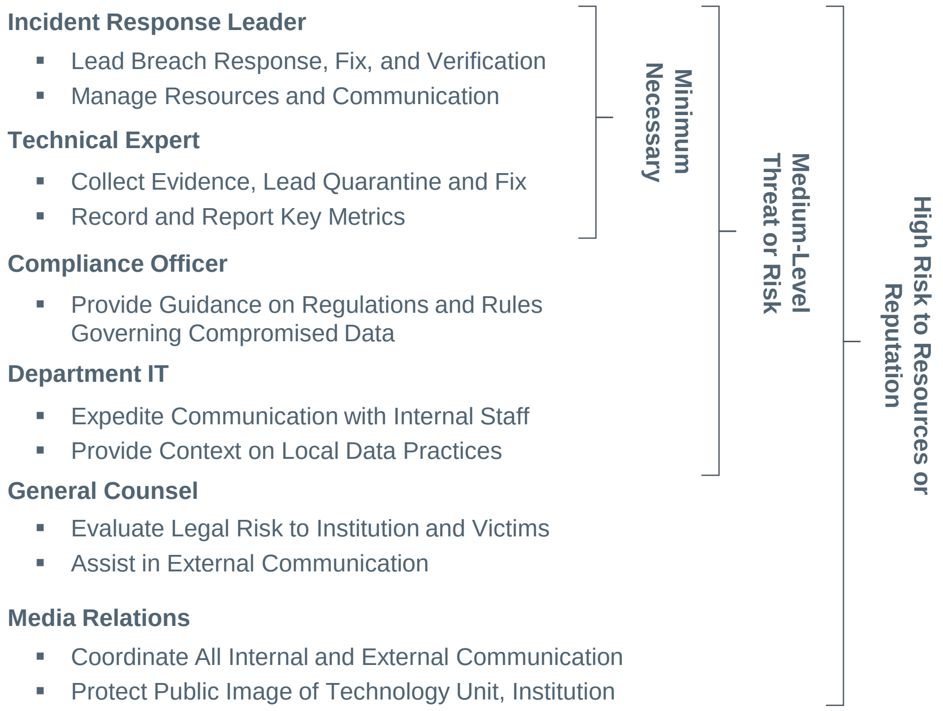
- *Document Key Facts:*
  - – Record date and time of breach incident, breach discovery, and when response efforts began
  - – Record who discovered the breach, reporting chain, and who on campus has been notified
- *Begin Assessment and Analysis*
  - – Estimate impact to institution and possible victims
  - – Prioritize response and notification components

A large team can slow response at a critical juncture, but too few participants can generate legal and reputational risk. Criteria that define initial steps and critical systems should build in recommendations for participation in the incident response team (e.g., type of impacted data, media relations, legal vulnerability).

Incident response leaders should prioritize capabilities above formal titles, and maintain a working knowledge of cross-departmental information technology functions.

Artifact D: See sample guidelines for a more comprehensive possible listing of incident roles (p. 17-21).

Escalate the Response Team With the Incident



Incident Response Leader

- Lead Breach Response, Fix, and Verification
- Manage Resources and Communication

Technical Expert

- Collect Evidence, Lead Quarantine and Fix
- Record and Report Key Metrics

Compliance Officer

- Provide Guidance on Regulations and Rules Governing Compromised Data

Department IT

- Expedite Communication with Internal Staff
- Provide Context on Local Data Practices

General Counsel

- Evaluate Legal Risk to Institution and Victims
- Assist in External Communication

Media Relations

- Coordinate All Internal and External Communication
- Protect Public Image of Technology Unit, Institution

Minimum Necessary
Medium-Level Threat or Risk
High Risk to Resources or Reputation

Source: Advisory Board interviews and analysis.