Department of Internal Auditing &OIT Incident Response Collaborative Model

Georgia Tech
Internal Auditing
206 Administration Bldg.
Atlanta, GA 30332-0254
(404) 894-9480
Fraud/Waste/Abuse Hotline: 404-894-4606

1 Event or Incident Requiring Collaboration

Critical incidents that require collaboration are incidents that extend beyond the borders of the local hardware or software system, and pose a threat of an adverse impact on the Institute's reputation, financial position, information systems security posture, or health and safety of faculty, staff and students. Examples of incidents requiring collaboration:

- Unauthorized access to sensitive information (e.g., SS#, credit card #'s)
- Suspected misuse of IS resources resulting in widespread compromise of information security
- Large scale intrusions

2 Ad-Hoc Group Convenes

- via phone or live conference

- Director of Internal Auditing
- Associate VP – Office of Information Technology
- Chief Legal Advisor
- Associate VP – Office of Human Resources
- Director of Information Security
- GT Director of Homeland Security

2a Other resources to be considered on a situational basis:

- Associate VP – Financial Services
- Director of Institute Communications
- Unit Head of Affected Area
- Chief Technology Officer

3 Ad-Hoc Group determines the resources necessary to reach a resolution on the incident. The Group will make the following assessments:

3a Is this incident likely to result in criminal or civil legal action?

If the answer is yes, the path below should be pursued. If no, 3b should be followed.

Scope:
A decision needs to be made to determine the point at which GIT will stop its internal investigation and hand it over to law enforcement and then to which law enforcement agency (e.g., FBI, GBI, Secret Service, and/or local law enforcement).

Review Method:
The standards of evidence for an investigation which is likely to result in criminal prosecution are far higher than those for which administrative action only is expected. For example, prior to any internal investigation of the machines involved, it would likely be appropriate to have law enforcement mirror the drives of machines, then turn the mirrored drives back to GIT for its internal investigation.

Investigation:
After coordinating with law enforcement, and preserving the integrity of the data on the machines, GIT will proceed with an investigation of the mirrored drives.

3b Is this incident likely to not result in legal action and likely to result in an administrative action that is localized within the Institute?

If yes, the following path should be pursued.

Scope:
A decision needs to be made at what level the investigation will take place and the standard of evidence that will be maintained. A decision will also need to be made regarding the point at which enough evidence has been obtained to satisfy the requirement to take appropriate administrative action.

Review Method:
The standards of evidence for an administrative investigation are less stringent than those which may result in legal actions but are important to maintain nonetheless. This ad hoc group must decide at what level evidence of the investigation should be documented.

Investigation:
As the internal investigation proceeds, the ad-hoc group must be cognizant of situations encountered which may change the examination from administrative to a potential legal investigation and take appropriate steps.

4 Assigning Investigation Oversight:

The ad-hoc group will determine which internal agency will take the lead for coordinating the investigation and communicating the results. This designated lead group will:

- Coordinate all efforts related to the investigation
- Determine the custodians of data
- Have responsibility for reporting results and ensuring continuing lines of communication

5 Conducting The Investigation:

The department or group with oversight of the investigation has the responsibility to communicate the results of the investigation, and ensure as soon as data on this incident relevant to the position of the Institute is uncovered, it reaches the executive decision makers.

6 Follow-up and Reporting:

The department or group with oversight of the investigation reconvenes the ad-hoc group at the end of the investigation and reports on:

- The outcome of the investigation
- Lessons learned (how the process worked)
- Cost of incident (in hard costs and personnel time devoted to the incident response)
- Discuss methods to prevent future incidents

11/14/2003