Anthony Gimei

Tabletop exercise.

1. What are common functions seen in various IR plans?
   1. Definitions of events, incidents, breaches.
   2. Roles and Responsibilities
   3. Classification of beaches
2. What business units are (or become) involved in IR plans?
   1. IT Help Desk
   2. Impacted Business Units
   3. Information Risk Management Team
   4. Office of General Counsel
3. In your opinion, what is the most critical function to “get right” in an IR plan?

The CAT (Contain, Analyze and Track) part is the most important part of the plan because if the plan does not get this right, it has the potential of paralyzing the entire organization. This helps the organization regain control after the incident and prevent it from spreading to other areas such as the network or the building or other systems.

1. Thinking back to our table top exercise, what was the most critical function needed in the plan?

The most critical function is properly classifying the incident (Critical, High, Medium, Low). This is because the correct classification with inevitably lead to assigning the correct amount of time and resources to resolve the issue. A properly resourced incident will be contained much quicker ensuring that the organization is least disrupted and that the cost of the incident is minimal.