Incident Response Programs
Questions Board Members Should Ask

Below are some questions you may ask management to ensure that the institution's incident response program is sufficient to allow the institution to satisfactorily respond to a cyberattack.

1. ***Does the institution's incident response plan identify an individual (internal or third-party) with the expertise to manage and coordinate all aspects of an incident?***

   WHY THIS IS IMPORTANT: Responding to a cyber incident can be chaotic, and time is often of the essence to ensure that the institution can successfully engage and work through its incident response plan. The incident response plan should identify an individual, either internally or through an engaged third party, who is well-versed and familiar with all aspects of the response process and can manage the complications that can arise from managing multiple teams of individuals performing different critical recovery duties. Although many individuals or teams will likely be carrying out separate duties during an incident, it is important that there is designated leadership for the entirety of the response process to ensure team coordination, inform management and the board, and address issues that arise in a timely manner.

2. ***Does the institution's written incident response plan address the following considerations:***
   a. ***Defined circumstances when the plan is to be initiated***
   b. ***Assignment of roles and responsibilities for individuals and teams identified in the plan***
   c. ***Notification thresholds for informing regulators, customers, and law enforcement***
   d. ***Escalation procedures for enacting business continuity/disaster recovery plans in the event of significant or long-term impacts to operations***

   WHY THIS IS IMPORTANT: The incident response plan itself can often be complex due to the many roles, responsibilities, and considerations it contains for management, operations, communications, and even technical response efforts. While a more comprehensive list of considerations is beyond the scope of this document (see the Incident Response Programs Fact Sheet), the considerations identified here define the circumstances for implementation of the plan when needed; who will be responsible for carrying out the plan when an incident occurs; when to notify regulators, customers, and law enforcement; and circumstances when enacting business continuity/disaster recovery plans becomes necessary to maintain continuity of operations during a significant incident.

3. ***Does management periodically test the incident response plan? Do tests involve individuals and teams with assigned responsibilities in the plan? Do testing efforts include senior management?***

   *WHY THIS IS IMPORTANT: **Periodic testing of the incident response plan** is an absolutely essential exercise to ensure that the program and plan are accurate, up-to-date, and reliable when needed most. Testing also helps to ensure that individuals and teams charged with responsibilities in the plan are familiar with their assignments. In the heat of an incident, well-trained personnel who are intimately familiar with the plan can reduce the likelihood that critical tasks are duplicated or forgotten altogether. Plan testing should address responses to a variety of incidents that the institution is most likely to experience and should involve all personnel with assigned responsibilities. In addition, testing events should ideally include senior management to ensure*

top-down awareness of response procedures, staff responsibilities, and general oversight needs in the event of an incident.

4. ***Does management ensure that the incident response plan is reviewed and updated when changes in vendors or staffing, the addition of new business units, or changes the institution's technology environment occur? Is the plan also reviewed and updated, as needed, following testing exercises and after real-world implementation of the plan? Does management track and remediate deficiencies identified from testing exercises, responses to real-world incidents, and changes in the institution's environment?***

   WHY THIS IS IMPORTANT: ***Changes in vendors or staffing, the addition of new business units, or changes in the institution's technology environment*** *are all events that necessitate a careful review of the incident response plan.* ***Experiences from real-world cyber events*** *also provide the institution with perhaps the most beneficial opportunity to update the incident response plan. Documentation of responses to an actual cyber incident (i.e., an after-action report) can cast a light on both strengths and weaknesses in the plan. Following an actual cyber incident, the institution should identify areas of the plan that require adjustment (e.g., stale contact lists for vendors and response team members, duplication of duties and other response process issues, etc.).*

   Any deficiencies identified from testing exercises, responses to real-world incidents, or changes in the institution's environment should be ***tracked, prioritized and remediated appropriately****. Management should make any necessary changes to the incident response program and incident response plan with appropriate urgency to ensure that they are ready to deploy immediately in the event of an incident - even if these modifications are necessary between normal policy review and approval cycles.*