COSMOS
Navigate the Compliance Universe

Compliance Today - July 2020
Considerations for incident response: What changes during a national healthcare disaster?

By Marti Arvin

Marti Arvin (marti.arvin@cynergistek.com) is Executive Advisor, CynergisTek, Austin, TX.

Most healthcare organizations perform drills for a variety of situations. It might be an airplane crash at the local airport, a hurricane or tornado hitting the local community, a major fire or earthquake, or a cyberincident, but those are all relatively local incidents. While healthcare organizations in the affected area may have issues, they can generally rely on the support of other nearby facilities. The preparation is not the same when the entire country is hit with the disaster.

Incident response is still something healthcare organizations must be prepared for even in the middle of dealing with a national crisis such as the COVID-19 pandemic. While the Department of Health & Human Services Office for Civil Rights has published its willingness to exercise enforcement discretion in a number of areas (e.g., telehealth),[1] it has not provided any indication that organizations can be lax in their incident response or breach notification. Many organizations have policies and procedures in place to detect, respond, and recover from an incident. A national emergency does not change this obligation, but the method of doing these steps may change when the entire organization is dealing with a crisis like the COVID-19 pandemic.

Healthcare organizations need to consider what changes they need to anticipate in their incident response when the assumptions they made for a local disaster are no longer valid. This article will focus on the response to a cyberincident, but some of the discussion will be relevant for other types of incidents as well. Prior to a national disaster like the current crisis, most organizations prepared to respond to a cyberincident by having an on-site command center. They may have also put in place a good vendor support structure. Ideally, the organization had strong tools in place to detect an incident and a methodology to assess if the incident resulted in a breach. But a number of these processes might need to be changed in a national emergency.

Changes to incident response communications

In considering incident response in an environment where multiple things are in flux, the organization is going to need to have contingencies in place to deal with the changing environment and a built-in flexibility to adapt as the circumstances continue to change. What COVID-19 has made organizations consider, hopefully, is how to deal with remote workers, how to access technology that may only be on site, the increased threat atmosphere, and the already extreme conditions staff are working under.

Often an outcome of an incident response exercise is the realization that the organization does not have good, up-to-date contact information for the key players who will need to be involved in the incident response. Being able to reach key players quickly and through means other than normal is important when an incident is unfolding during routine operations. This is critical when the entity is operating with a significant number of the workforce working remotely.

Many organizations think about and gather contact information for their key internal stakeholders but don't always keep it up to date or in a location that can be easily accessed during an emergency situation. Most have not

considered, even with a current contact list, the implications of contacting and coordinating communication between stakeholders when most are working remotely (e.g., what the implications of poor cell phone connections, internet bandwidth issues, or conference line capacity issues are).

Employees may find it strange to go from commuting to an office every day to commuting to the home office. And that "home office" might be their bedroom, kitchen, or living room. In a crisis, it may be necessary for individuals to be on conference calls or video chats during nonstandard hours. If that home office is the living room or kitchen, what are the implications to the individual's home life? This may make it more difficult to have an effective dialogue with everyone. It may also be more difficult for the individual to focus on supporting incident response.

During an incident, there is often a command center set up, and key players operate out of one location. It makes it easier to communicate and allow more than one conversation at a time. However, when everyone is on a conference line or video chat, that becomes difficult. This can also extend the time to get response and recovery measures in place.

Another often-overlooked group for having up-to-date contact information is vendors. This may include vendors needed for the response, such as the organization's cybersecurity insurance company, outside counsel, forensic experts, information technology (IT) partners, and breach response support vendors. This may also include key business partner vendors who need to be alerted that normal access to the entity's systems may be interrupted.

Organizations should reach out to vendors who are key to supporting their incident response and get multiple good contacts for each vendor. It may also be important to understand the vendors' constraints. Ensuring that each vendor has a contingency plan to support the needs of the facility experiencing the incident is something to consider before the incident occurs. It might be necessary to look at other vendors if the vendor of choice does not have the capability or if the healthcare entity is not comfortable with the contingency plan.