**Compromised Business Partner**

The majority of healthcare organizations do not conduct 100% of their business operations entirely in house and commonly rely on business partners for functions like billing and a host of other business functions.  While the HITECH Act has improved the security and privacy practices surrounding business partners with the introduction of BAAs, there is still the likelihood that at some point a business partner may become compromised and as a result, can be used to attempt to compromise the hospital in a manner similar to what Target experienced with its HVAC vendor.  Likewise, a compromise of a vendor that the hospital exchanges data with may also mean that there is the potential for the hospital to suffer a data breach via breach of its business partner. This scenario will highlight some of the security issues that hospitals face via their business partner associations.

# Start of the scenario:

The hospital makes use of a remote radiology service for the reading of x-rays, CTs, MRIs, and other medical images for after-hours cases and to supplement their in-house radiologists during the day. At 4am on a holiday weekend this radiology service is the sole source of coverage for the reading of hospital radiology images. At that time, the hospital notices that none of their images appear to be crossing over to the remote vendor and none of the reports from that vendor appear to be coming in to the hospital’s EHR. To make matters worse, shortly after this discovery a patient is delivered to the emergency room with a suspected stroke and the hospital will now urgently need to have a CT scan read in order to determine if a tPA treatment is needed. There is only a limited window of time to make this determination before permanent stroke damage becomes more probable.

## Questions to consider:

1. How will the clinical challenge of being unable to read a stroke patient’s CT scan be dealt with?
2. What is the downtime plan for a remote clinical service which goes down?
3. How long will that downtime plan take to be put into place? Will it meet the needs of the stroke patient?
4. How long does your downtime plan extend for? If this outage last for more than a day does your downtime plan cover that?
5. What troubleshooting steps would be taken at this point?
6. What is the procedure for escalation with the vendor and escalation with internal IT?
7. What kind of SLAs were negotiated for this service? Do they meet the stroke patient’s clinical needs?
8. From a technology perspective, what are some of the initial tests or inquiries to be made to the vendor’s IT team in order to assess the problem? What about the EHR?

# Inject 1:

About 8 hours later services appear to be restored and operations are back to normal, however the hospital CEO receives a notification that the remote radiology vendor suffered a cyberattack which lead to the outage. As a part of the cyberattack, there is a change that PHI pertaining to hospital patients may have been accessed. The letter informs the CEO that a forensic investigation is currently being done and that the hospital will be notified if PHI was actually accessed within two weeks’ time.

## Questions to consider:

1. Does the hospital have a BAA with this vendor? What contractual obligations does the BAA place on the vendor?
2. What other contracts are in place with the vendor? Do any clauses in these contracts apply to this situation?
3. What kind of security and privacy due diligence was performed in onboarding this vendor?
   1. Were SOC2 reports, HITRUST reports, or other independent audit information obtained?
   2. Was the vendor reviewed by the security department before the contract was signed?
4. How often is security and privacy due diligence performed against vendors that are already onboarded?
5. What actions should the hospital take to prepare for the possibility of a breach having occurred with this vendor?
6. What are the key stakeholders within the hospital that should be notified of this potential incident?
7. Does your cyberliability insurance potentially cover the costs of remediation or of notification?

# Inject 2

Two weeks pass and the CEO gets another notification from the vendor that the company was indeed breached and PHI pertaining to 1,500 hospital patients had been accessed. The notification explained that the radiology reading service made use of a public cloud provider to host the PACS system used by the firm’s radiologists. It was this PACS system that was attacked and breached and not the radiology reading firm directly.

## Questions to consider:

1. Does your BAA and/or other contract language cover breaches of 3rd parties to your business associate?
2. Does a hospital cyber-insurance policy (if any) cover breaches of business associates or just the organization directly? Does the policy cover breaches to 3rd parties of your business associates?
3. What are the hospitals reporting responsibilities?
4. How will public relations and other media inquiries that may result from reporting be handled?
5. How will affected patient notification be handled?
6. How will the hospital reassure patients that the hospital is still safe to use, despite this breach?