**Lost/Stolen Laptop/Smartphone**

Healthcare organizations routinely allow their employees to work and access data remotely. Management and other key personnel have organization-provided laptops/smartphones assigned to them that can contain a certain degree of company confidential information or, worse yet, PII or PHI data.

In this scenario, we aim to think through the ramifications of a lost/stolen laptop or smartphone. In most cases there are no distinctions between the two.

# **Start of the Scenario:**

At 9:37 AM, the IT department receives an urgent request for a replacement laptop for the VP of Finance. Details on the whereabouts of the original laptop were not provided as the call was initiated by his/her administrative assistant. The IT support technician was not able to press for details as the assistant did not have any and the VP was in meetings all morning and unavailable to take calls. Due to the urgency of the request and seniority of the executive, the help desk proceeded as if the existing laptop malfunctioned and that the user did not wish to go through any troubleshooting steps.

## **Questions to consider:**

1. Would the InfoSec team be notified of a potential loss of equipment, or would it be assumed that the equipment is still in the control an authorized person?
2. Are there controls in place to keep data safe even in the event of equipment being lost/stolen (e.g. an MDM)?
3. Who is responsible for device security? Is there a centralized list of devices and security products installed on each device?

# **Inject 1:**

1:50PM, a different IT support technician gets a call that the “cellphone of the VP of Finance is also missing.”

## **Questions to consider:**

1. Would a connection be made that a request for a laptop was initiated earlier in the day and that now the laptop is potentially missing?
2. Would InfoSec team be notified of potential loss of equipment?
3. Is there an available inventory of potential data present on the laptop?
4. Is the laptop encrypted? Does the department have the ability to remote-wipe the devices?
5. Is there an emergency contact for the authorized user so that the team can reach the user? What if his/her smartphone is also missing?

# **Inject 2:**

2:17PM, the IT support personnel decided to track the smartphone. The device’s last known location is 7 hours old and is not consistent with the authorized user’s known home address or work locations. The authorized user is still unavailable; however, his/her assistant confirms that they don’t know the whereabouts of the laptop/smartphone.

# **Questions to consider:**

1. What steps would be taken?
	1. At what point would a remote wipe be considered appropriate?
	2. At what point should the VPs meeting be interrupted and he be forced to make himself available?
2. What is the risk? What information could be compromised?
3. What available options do you have to mitigate the risk?
4. Does the seniority of the person who held the equipment impact the mitigation needs? Should a laptop lost by a nurse be treated the same as a laptop lost by a CXO or Board Member?
5. Does the location of the lost device impact how the situation is handled? Would it be handled differently if it was found to be sitting in a local coffee shops vs the airport vs a foreign country from recent travel?
6. Who is responsible for mitigating the risk, what procedures do you have in place to mitigate this risk?

# **Suggested repeat with a twist:**

Walk through the same scenario again, but this time with the authorized user initiated the call and says that he/she left her laptop bag at the airport last night. Does this information change any of the answers above? Does it change your response strategy? Is your assumed information disclosure risk initial assessment higher/lower than the initial scenario?