# Partner Incidence Response (PIR)

# Data Breach

- Fill out IPIH-Identification Form
- DO NOT ALLOW THE CLIENT TO POWER OFF ANY COMPUTERS.
- Note any important timestamps – first detection of the event and what triggered it.

Schedule Onsite – Tech must bring "Forensics Go-Bag"

Tech must have: Write Blocker, External Evidence Drive, Chain of Custody Form, IPIH Survey Form, IPIH-Identification Form, and basic tools for removing hard drive

1. Identify Point of Entry – (if possible)
    a. Open RDP Ports? If so, where are they going?
    b. Server logs – External Authentication? To what machine?
    c. 3rd party remote access tools? (Logmein, GoToMyPC, etc.)
2. Proceed to Imaging Patient Zero and Server (OS drive only)
3. Using MagnetRAMCapture.exe, create a RAM Dump (included on USB Drive)
4. If the computer is a workstation without RAID, skip to 11. If the client demands that the hard drive not be removed, continue from 6 and skip 10. YOU MUST ADVISE CLIENT THAT CHAIN OF CUSTODY WILL NOT BE MAINTAINED AND MAY AFFECT ANY COURT PROCEEDINGS IN THE FUTURE.
5. If the computer is a server with RAID, continue to 6 and skip 11
6. Using FTK Imager – Create Disk Image (included on USB Drive)
    a. FTK Imager > File > Create Disk Image > Physical Drive > Select Drives > Add Image Destination > select E01 >Fill Out Form > Destination=External Evidence Drive > Image Fragment Size=0 > compression=6 > Finish > check verify and start.
7. Fill out IPIH-Survey Form
8. Fill out Chain of Custody form – include hard drive info (Patient Zero)
9. Case number should be company-date MMDDYY (ex. Stetson-050818)
10. Evidence number should be Company-Item-MMDDYY (ex. Stetson-JWHDD-050818)

11. Remove HDD from Patient Zero and label it with the evidence number
12. Submit to Stetson for full investigation – ALL HARD COPIES OF FORMS STAY WITH EVIDENCE AT ALL TIMES

- If client insists on not installing a new, clean HDD with clean install, a disk clone will be done and the clone will be returned after cleanup.
- ORIGINAL HDD MUST BE SAVED!
- Write Blocker must be used at all times on original evidence to maintain chain of custody.