horizontal line

**Plus971 Cybersecurity**

Report on Investigating employee fraud in a bank

**21st August 2023**

**What diplomatic strategies should you use?**

* **Open Communication:** we need to create open and honest/transparent communication between our firm and relevant personnel at the bank such as the network admin and the relevant management, we will achieve this by not dodging emails or questions and answering them to the best of our knowledge at the time maintaining trust throughout the investigation.
* **Respect for Operations:** We will do our best to respect the bank's operations as it directly deals with people's welfare and the public's perception of the company. Our investigation must be as minimally invasive as possible to not cause disruption to normal day-to-day operations.
* **Privacy Protection:** our team will not disclose any person’s financial data, PI or SPI, we will handle all sensitive information securely with confidentiality as a leak of this information could lead to identity theft, loss of assets unjustly, fraud, etc....
* Furthermore: this investigation will only analyze the activities of the employees, not any customers’ activities unless it is directly related to the case.

**Which acquisition method should you use?**

* We should use an over the network data acquisition method as there are 4, 20 TB Machines which are already networked and performing data acquisition onsite would require moving computers to and from the site, with a LAN based approach we can acquire the data remotely.
* We can mount the network drives as shares in our forensic lab computers and use imaging software such as FTK imager which can image drives over the network.
* While an on-site acquisition is very much possible it is not advisable as the cloned hard drives would need to be transported in such a manner as to not destroy the read/write head and the platters, it would also include the risk of the drives being stolen which could lead to the privacy protection problems we discussed in the section above.

**Expected Problems:**

* **Data Acquisition:**
  + Problem: Customers or bank officials may have an issue with transferring data that is confidential but not necessary for the investigation being transferred to our lab.
  + Solution: We only take data necessary for the investigation therefore addressing the diplomatic strategies and keeping traffic disruption to a minimum.
* **Data integrity Verification:**
  + Problem: how can we ensure that the data we collect from the banks servers have not been tampered with after the transfer by our forensics team, thus making the evidence we collect not admissible in court?
  + Solution: Create not 1 but 2 hashes of the data on the bank’s servers (SHA1, MD5, …), and after the transfer to our servers and our investigation, we can run the same hashing algorithms and verify data integrity
  + Another Solution: We use software based write blockers to not mistakenly change the data in those files.
* **Network Traffic Impacts:**
  + Problem: As we will be transporting large volumes of data this could trigger any bank security measures such as an IDS/IPS (Intrusion Detection/Prevention System).
  + Solution: We coordinate with the bank’s network admin to account for the network transfer caused by the data transfer
  + Another Solution: We do the data transfer when the bank’s network is experiencing off-peak hours.
* **Over The Network Data Acquisition Security Concerns:**
  + Problem: Exposing a network share over the internet no matter what protocol it uses i.e., SMB, FTP, … is not a good idea as this can lead to data being stolen.
  + Solution: We use a VPN to allow both the bank’s servers and our forensic lab to transfer data, all communication will happen through this VPN, and we close the connection to the bank's servers when we do not need to use it.