Technical Concerns:

* Lack of a Host-based Intrusion Prevention System
* Malware was able to infect system when employee connected to networks through VPN
* VPN servers had two-factor disabled
* Poor network segmentation of critical digital assets

Human Behavior:

* An employee installed malware on a personal computer and then connected to company networks through a VPN

Business Decisions:

* Two-factor authentication disabled on company servers, even after an update to enable it
* Lack of employee security awareness training

I believe the most crucial factor which led to the J.P. Morgan security breach was their business decisions. As we have seen in many case studies thus far, humans are indeed the weakest link when it comes to cyber security. Which is why J.P Morgan should have dedicated a larger portion of their security $250 million dollar security budget focused on training their employees and bringing awareness to how an employee’s actions can affect an origination's security. Another unwise decision was to not have policies in place to check if two-factor was enabled and working on all company servers after their update. The importance of having multiple factors to prove one's identity is vital to protecting personal identifiable information inside an organization. This attack is so significant because even if a company spends $250 million dollars a year on security, it does not guarantee safety for their digital assets.