# Homework 1

The capital one incident under review in this article goes over how an individual was able to hack into their AWS server and exfiltrate much of their data onto a local machine they were using. The article covers the guidelines that capital one was using and how in the US it is up to the company’s interpretation to fulfill such guides. Then it breaks down what lead to the attack

To be such a large company and to be missing devices such as IDS and IPS’s on your network or storage solutions is a little crazy to me. In my head these devices would be a bare minimum. And do to a lack of including the least privilege principle as well, which I feel was taught in CS classes near the first week or at least the first semester and iterated in every class since.

This all made me think of a discussion from the other day from the differences of Europe’s guidelines compared to the US’s and how the latter are way worse. This made me think if this was a Europe company how would those guidelines look different or how would it have led to a different implementation of security from the companies point of view and would it have prevented such things from happening.