Case Study: Target Corporation

Technical Concerns:

* Point of Sale terminals were vulnerable to RAM scraping malware
* Anti-intrusion software only gave warnings, did not quarantine identified threats
* Network did not isolate sensitive information

Human Behavior:

* Target’s security team ignored the warnings from their anti-intrusion system during malware installation
* Targets security team ignored warnings from their anti-intrusion system of the escape routes the attackers planned to use to extract data from their network

Business Decisions:

* Gave access to a small third-party vendor that did not have strong information security practices in place
* Lack of information security policies in place to have sensitive information in their networks isolated

In my opinion, I believe that the business decisions are the most significant factor. A company of Target’s size should have no problem with demanding their third-party vendors be up to industry standards. In my opinion, it’s negligence on Target’s part for not doing a proper security audit with their partners and addressing any concerns before giving them access to their networks. Another egregious decision was to not have policies in place to ensure that sensitive data such as a customer’s personal information be isolated from other networks. Their customers privacy should be one of the most important aspects of their business, but this case study clearly shows otherwise. I almost went with the human behavior as the most significant factor because the lack of response by their security team, but I believe if the proper policies were in place, they could have mitigated the damage done significantly. It’s no wonder why this attack was a catalyst for the current chip readers, because looking at it from a first principles perspective, it solves the problem at the ground floor instead of depending on companies security policies.