**Why are some businesses so nonchalant about cybersecurity?**

Two reasons come to mind - lack of knowledge and cost. Often, the people in charge of a project don't even know how to create a folder on their desktop. They were put in a position of leadership for one purpose and one purpose only: make money for shareholders. If someone on a dev team was to suggest putting in more time to iron out security vulnerabilities, the answer is most certainly no as time = money.

**What is the corporate thought process when trying to balance good engineering practices and profitability (i.e., new features)?**

Corporate thought processes often do not involve balance. I firmly believe that all decisions based on "engineering practices" boil down to "how much revenue can we generate from this" and "how much money can we save"

**What mistakes in the engineering world lead to the most security vulnerabilities? Why is this the case?**

For engineers, I believe time is the biggest factor. Engineers often are put under insane pressure as the tech world continues to tighten deadlines and their co-workers continue to be laid off en masse. How does one have time to hunt for vulnerabilities when it's impossible to get the feature out in the first place?

**Where along in the human-computer interaction are the most vulnerabilities found – that is, where do a business’ employees fall victim to social engineering attempts?**

This goes back to my point on lack of knowledge. If a user is unable to operate a computer beyond the simplest of tasks, how are they to determine a fake login page vs a real one?

**Why wouldn’t a business or corporation invest more heavily into cybersecurity?**

Why would they? Training people costs money. Fines and regulations for leaking customer data is so miniscule it's laughed off somewhere in the budget. Sure, some sort of ransomware could destroy a company, but do you really expect the higher ups to understand the weight of that statement? I can't remember how many times I've heard "Well, I had an antivirus, why didn't it protect me?"

**What can be done to stress the importance of such an effort to stakeholders and decision makers?**

Put it into terms they understand. Money. Show them case studies of much money the average cyber attack can cost.

As a part of the bigger picture, I believe that fines / regulation for companies allowing customer data to be leaked should nearly put a company into financial ruin.

These two points together would significantly reduce the amount of cyberattacks we see and protect our data from falling into the wrong hands due to circumstances outside of our control.