Effects of Different Pain Relievers and Dosages on Cognitive Retention

Navya Hooda Mohammed Yusuf Shaikh Shivank Goel
Vanshika Vanshika Jena Shah

February 27, 2025

1 Introduction

Therefore, in response to such attacks, there is a need for a plan, that not just keep the intruder or hackers out but also quickly alert if an attack does happen. Our study looks at cyber resilience, which is " the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." as defined by National Institute of Standards and Technology [@NISTGlossary2023]. We break our study into three major research questions, which forms the thesis of our study:

RQ1: How do organizational factors such as size and sector, influence the severity of cyber breaches experienced by companies?

RQ2: Which cybersecurity strategies, including frameworks, policies, and preventive measures, are the most effective one, in reducing the damage caused by cyber attacks?

RQ3: In what ways do the industry type and digital dependence of a business affect the overall impact of a cyber attack, in terms of preserving confidentiality, integrity and availability of data?

We also plotted a bar graph **?@fig-sector** to count the number of incidents across various sectors. The bar chart clearly indicates that the 'Human Health Activities' sector has the highest count of incidents, standing out significantly from the other sectors. This might suggest that health sector is a more frequent target for cyber incidents or probably it is more diligent in reporting such events. The other sectors show a range of incident counts, with most appearing to have far fewer incidents in comparison. This could point to different levels of risk exposure, varying security measures, or reporting practices across these sectors.

2 References