Approaches of Data Security by Businesses

WINONA STATE UNIVERSITY
Computer Science Department
http://cs.winona.edu

Peter Schurhammer
Dr. Ming, Ma and Dr. Iyengar, Sudharsan

WINONA STATE UNIVERSITY
Computer Science Department
http://cs.winona.edu

Introduction

- Every 2 seconds someone is a victim to some sort of identity theft or data breach (add reference here). That roughly makes up 118.6 million people in the first half of 2021, costing a total of $56 billion according to the Federal Trade Commission.
- The leading statistic for these claims primarily come from fraud complaints with actual identity theft complaints doubling from 2019 to 2020.
- The key importance of this protection and analysis is to help give individuals the foresight to keep these sorts of breaches avoidable.

Hypothesis

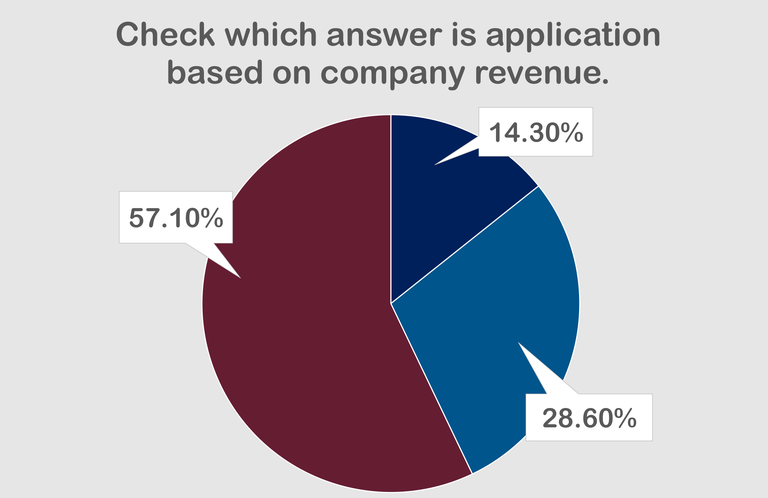
- The hypothesis would be that different companies will have different variations of the same security practices. Meaning that they might have different naming conventions or even different layers, but will all generally be relatively similar.
- Companies utilize similar data protection techniques across size, industry, and geographical locations.

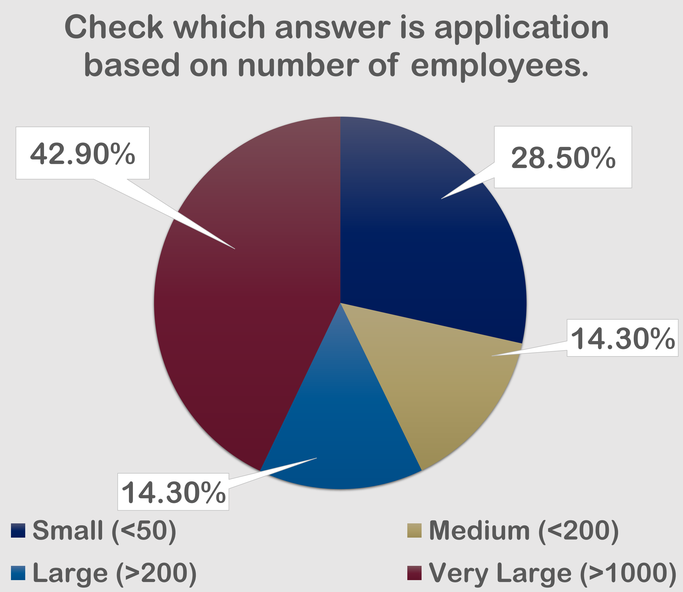
Methods

- My methods for answering or testing my hypothesis would be survey both private and professional businesses and individuals on their strategies for preventing malicious attacks. This would be by asking a preapproved set of questions to each party involved and then recording their responses.

Results

- Based on this study, there is a wide range of techniques that people can use to breach data maliciously. Results from this study indicates that every individual surveyed was worried about potential security risks in their company, independent of the size and scope of the business.
- Involved in the survey the is the use of techniques and tips to help prevent such breaches from even happening. A significant response from the survey was “keeping up with infosec and maintaining up-to-date versions of tools and platforms.” Results indicate that there was at least one layer of security used; with only one response without any security.
- There were three responses with two layers, and seven responses with two or more layers of security.





Some Responses From Survey

- **QUESTION**: What sort of techniques or tips, if any, do you have for those trying to prevent breaches and bolster security?
  - “I think that when designing any professional application it is good to have a security requirements design meeting to identify where breaches could occur. As developers we can prevent them all but we can try.”
  - “make security easy and automatic for users to use. for example, when our company increased passwords requirements, they gave us all password managers for work and personal use.”
  - “Develop with security in mind. Always use the internet basics, HTTPS, TLS 1.2+, OAuth, etc. Always keep up to date on any 3rd party libraries being used.”

Conclusion

- In conclusion, results from the survey shed light on how individuals in different sized companies think and react to cyber security risks and issues.
- It also gives examples how of these individuals think and cope with the ever-present danger that comes with their data possibly being breached as well as how equipped their employers are with dealing such breaches/attacks.

References

- https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
- https://enhalo.co/why-cybersecurity-important-for-modern-day-society/
- https://www.upguard.com/blog/cybersecurity-important
- https://www.techtarget.com/searchsecurity/definition/cybersecurity
- https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams