CPSC253 – Cyber Security Fundamentals and Principles
Project Guidelines

Introduction

You are a Senior security consultant for BizSecure, a up and coming security firm that offers consultancy services for businesses. Among the services the company advertises is an offering that includes a comprehensive security analysis of the client's business, coupled with a detailed report on the findings along with BizSecure's recommendations.

For the next three weeks, you have been assigned to provide this service to MediDoc Inc., a medium sized business that specializes in handling medical insurance claims and paperwork.

MediDoc's customers include medical practitioners (physicians, dentists, etc.) and local hospitals who outsource their medical insurance claim process to MediDoc.

Background

MediDoc Inc., has been in business for just over two years and has enjoyed double digit growth in YoY (year over year) revenue for the past two quarters. They have grown their customer base by a staggering 88% since the beginning of the year. With the sudden increase in business as well as publicity, MediDoc's Chief Technology Officer Tom Zeigler can't help but think about securing the digital records the company handles. Fortunately, MediDoc has yet to have a security incident – Zeigler wants to keep it this way.

You have interviewed Zeigler and collected information on MediDoc's current state of business. The following describes the company's demographic, services, assets/infrastructure, etc.

Demographic

- 250 employees
    - 150 full-time, 50 part-time, 50 interns
    - 10 executives, 80 salespersons, 90 insurance specialists, 20 in accounting, 50 in IT department
    - The sales staff are mobile and work remotely 90% of the time
    - Insurance specialists, accountants, and IT staff work strictly on-site in the office
- Office located in Central California, in Pismo Beach

Services

- OneAuth – Centralized identity provider that manages customer's as well as MediDoc employees' login credentials and access to software
- SureFile – Claim filing software that MediDoc's insurance specialists use to electronically file claims for patients
- Quickbooks – Accounting software for the company's finances

Assets/Infrastructure

- Authentication server (OneAuth)
    - Hosts Identity and Access Management software
        - Accesses granted manually after new user is on-boarded
        - System admin maintains and operates the software
    - On-site database stores both employee and customer credentials and profile information
    - No redundancy (backups)
- Application server
    - SureFile – accessible with login credentials regardless of network access
        - Contains PII (Personally Identifiable Information) and health data in an application database
        - Locally hosted
        - No redundancy (backups)
    - Quickbooks – accessible with login credentials regardless of network access
        - Contains customers' billing information (bank account, credit card, invoices)
        - Locally hosted
        - No redundancy (backups)
- Laptops, company-paid mobile phones
    - Mostly used by the sales staff
- Servers and storage
    - Servers and databases that host MediDoc's services and data

Current State of the Business

Tom Zeigler has given you insight into the business operations. The following is a list of relevant notes that you have compiled which may help in assessing the situation in more detail.

□ The System Administrator is the single point of contact for granting access to company assets.

□ MediDoc's customers (physicians, dentists, hospitals) send unencrypted patient documents through email or upload to MediDoc's cloud storage (e.g. Dropbox)

□ Sales staff is constantly on the road and tend to rely on public WiFi

□ MediDoc may be a target for cybercrimes (e.g. DDOS, SQLi, Viruses)

□ There does not exist any mitigation or recovery plans in case of failures or breaches

Deliverables

3 – 5 pages (excluding cover sheet and/or references), single spaced report.

Layout of the report can be organized to your liking, but **must include**:

- Executive summary
- Introduction – describing the context and purpose of the report
- An analysis of potential problems / threats that were determined
- Recommendations / follow-up actions and the reasoning behind decisions (can be specific)
- References (MLA format) for outside research done

The report can also include:

- Diagrams
- Outside research

You are free to make reasonable assumptions on matters that are not described.
Any of these assumptions made must be documented.

Rubric

Category	*Points*
Comprehensiveness Did you address MediDoc's concerns?	40
Validity Are your recommendations legitimate?	40
Presentation and readability Is your report well-written? Is it presented in logical order? Is it engaging?	20
Total	**100**