ARAIZ NAQVI

SECURITY ASSESSMENT

Sky Media

07TH OCTOBER, 2024

2024-2025

ARAIZ NAQVI

TABLE OF CONTENT

2024-2025

ARAIZ NAQVI

DISCLAIMER

This incident report is a project-based simulation for the fictional organization *Sky Media*, as part of the "Fundamentals of Cybersecurity" course on Google's Coursera platform.

While the details may resemble real-world scenarios, all data, systems, and findings are entirely fictitious and created for educational purposes. This incident report does not reflect any actual incidents or vulnerabilities affecting any real organization, including *Sky Media*.

Though based on practical analysis and protocols, the assessments are conducted in a simulated environment and should not be considered representative of any real entity's security posture.

2024-2025

ARAIZ NAQVI

INCIDENT OVERVIEW

Date of Incident:	2024-10-05
Summary of Incident:	The organization Sky Media recently experienced a major data breach, which compromised the safety of their customers' personal information, such as names and addresses
Nature of the compromise -d data:	Most likely PII's, with small possibility of SPII's.
Reported By:	Araiz Naqvi
Reported On:	2024-10-07

ARAIZ NAQVI

IDENTIFIED VULNERABILITIES

Password Management:
Potential easy to guess passwords with no followed security policy or standard guiding them. Also, large scale password sharing prominent.

Database Security:
The database security is weak, with default passwords still in place. Additionally, regular security audits are not conducted, and admin access credentials are not periodically rotated.

Firewall Configuration:
Firewalls are not up to date. Plus, there are no strong filters set to control incoming and outgoing traffic. Additionally, traffic is not monitored and logs are not maintained.

Multifactor Authentication (MFA):
No MFA in use. Also, no regular MFA policy audits.

2024-2025

ARAIZ NAQVI

NETWORK HARDENING TOOLS AND METHODS

Encryption using the latest standards:
Encryption used to conceal outgoing data and uncover or Decrypt the incoming data.

Firewall maintenance:
Includes checking and updating security configurations regularly to stay ahead of potential threats by keeping an eye for incoming and outgoing requests.

Multifactor authentication (MFA):
A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.

Network log analysis:
The process of examining network logs to identify events of interest.

(PTO)

2024-2025

Password policies:
The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords.

Server and data storage backups:
Server and data storage backups help protect data assets from being lost. Backups can be recorded and stored in a physical location or uploaded/synced to a cloud repository.

Araiz Naqvi

Network Security Engineer

If you find this helpful, you'll love my content!

@araiz-naqvi

@araiznaqvi