Title Analyzing Major Cyber Attacks in 2024 by Ubong Etim

HEALTHCARE

1. Change Healthcare:

Change healthcare was subject to the largest data breach/cybersecurity incident affecting the healthcare industry in 2024. Some of the important information about this incident:

Date: Change Healthcare's systems were infiltrated on 12th February 2024 and critical files were encrypted on the 21st of February 2024.

Mode: The attack was carried out by the BlackCat group using ransomware which exploited a citrix portal that lacked multi-factor authentication.

Impact: Change healthcare paid a $22 million ransome and suffered a prolonged outage which caused a halt in services which affected revenue cycles of healthcare providers that use(d) their systems. They were also subject to an exit scam and multiple exploitation attempts.

Remediation: Change healthcare disconnected other services to prevent more compromise of data, they enlisted the services of professionals to rebuild their cloud based systems with emphasis on implementing multi-factor authentication.

2. Ascension Health:

Date: Ascension health's cyberattack was discovered on May 8th 2024.

Mode: Ascension health was one of the victims of the Black Basta ransomware attacks responsible for the disruption of services across 142 hospitals. The initial attack vector was a malicious file that was downloaded by an ascension health employee.

Impact: The disruption of services affected electronic health records and lasted 4 weeks, compromised some of its servers and exposed the data of about 5 million patients.

Remediation: The remediation efforts focused on customer notification and support as well as network isolation and a slow but gradual system restoration.

FINANCIAL SERVICES:

1. **Snowflake :** American cloud based data storage platform.

Date: Snowflake's cyberattack took place and was discovered in April 2024.

Mode: malware was used to gain access to user credentials and accounts that lacked multi-factor authentication were exploited.

Impact: At least $500,000 in lost revenue, stock price fell by 5% highlighting reputational damage and lawsuits/litigation, exposure of potentially sensitive customer data as it was a third party or supply chain exploit that affected multiple customers of snowflake.
Remediation: Remediation efforts focused on customer notification and support as well as enlisting the services of companies like Mandiant to diagnose problems and prevent future recurrence.

2. Patelco credit Union:

Date: The attack took place on June 29 2024 and was reported on 2nd July 2024.
Mode: It was a Ransomware attack as a result of a phishing email.
Impact: two week system downtime compromised and exposed the data of more than 500,000 customers and employees.
Remediation: collaboration with the department of financial protection and innovation to ensure more robust cybersecurity measures were implemented, customer updates and and support were also some of the measures taken.

RETAIL AND E-COMMERCE:

1. **PandaBuy:** Chinese E-commerce platform.

Date: the cyber attack was disclosed to the public on 31st March 2024.
Mode: It was a Ransomware attack that stole user data and put it up for sale.
Impact: Exposure of the data potentially belonging to millions of customers as well as ransom and multiple other attempts at extortion.
Remediation: Communication with customers and comprehensive security audits.

2. **Lookiero:** European Online styling service.

Date:It was discovered on 20th March 2024, and was disclosed to the public on the 20th of August 2024.
Mode: A Ransomware attack.
Impact: Exposure and compromise of the data potentially belonging to over 4 million customers.
Remediation: Limited public disclosure regarding response.