**A04 Feb 6 ClassNotes and Data Breaches Presentation**

Banks typically know a lot of personal information.

* In thailand 49% of banks use machine learning for fraud detection
* SAS service, use machine learning models from kafka
* Anomalies in spending habits, spikes in purchases, large transactions, location change, could all contribute to detection.
* A common fraud case in southeast asia is money laundering and gambling. They make use of people to make host accounts.
* Data retention policy, 6 years
* Hard disc data are disposed of with lasers to entirely rid of information

Problems created by AI

1. Machine learning biases
2. 2 types of data can be abused by AI in finance

* **Data coming from geographics and data coming from demographics**
* Leads to unfair
* Cards all full, strange IP. The moment AI sees his cards are full, AI will detect
* 2008 caused an apr spike because of home loan scams
* Biases can come from demographics. Age, sex, race.
* Bias in unavoidable
* Anti bias AI; is it possible?
* Bias is decisions based off opinion
* **Data coming from card usage data.**
* Data can be used for different things.
* EX; using card usage data to market. Like offering someone
* Card usage data can be abused by AI too.
* EX; keeping track of spending habits to deny people of rights because AI bias has led it to assume a user is a dangerous user. Or someone with hospital bills being denied a home.
* Card using gives away a LOT of information.

2. Lack of transparency

* No longer just determined with credit score, also credit worthiness

1. Data breaches

* Usually financially motivated and 100% caused by use of technology.
* Data security and confidentiality have been compromised

Lots of companies have been victims of API scraping

* Read about crowdstrike patch breach
* Fully AI automated patch system was compromised. They lost 5 billion dollars

What percent of last 10 years data breaches have happened, why do most of them happen and how could they be solved by AI? What root problems, techniques for remedial action. Looking into finance

Financial industries are one of the biggest targets for data breaches. In the past 10 years, nearly 40-50 percent of all data breaches have been finance related. Here are some fun facts: some of the most significant data breach statistics pulled from the list below:

* By 2025, the global cost of cybercrime is projected to reach $10.5 trillion, growing at a rate of 15 percent annually.
* The average cost of a data breach reached an all-time high in 2024 of $4.88 million, a 10% increase from 2023.
* Nearly half (46%) of all breaches involve customer personal identifiable information, which can include tax identification numbers, emails, phone numbers, and home addresses.

This usually comes from financial institutions vulnerable to phishing attacks, malware, insider threats, and vulnerabilities in outdated software. Things are changing, computers are being trained to be smarter, and certain institutions do not keep up. A lot of these problems are rooted from weak security protocols, lack of phishing awareness, inadequate multifactor authentication, and insufficient user data monitoring. AI can help with anomaly detection to monitor behavior, and predictive analysis can also help detect new vulnerabilities by analyzing historical data and coming up with potential future threats.

A specific case:

* **Targeted**  **JPMorgan** **Attack:** JPMorgan Chase was hacked by cybercriminals in October 2014, allegedly from Brazil.
* **Root Access:** Attackers gained root access to over 90 servers.
* **Minimal Data Stolen:** Only customer contact info (names, emails, phone numbers) was taken.
* **Attack reason:** Likely for future phishing or targeted cyberattacks, not financial theft.
* **Compromised Data:** Internal login details and customer contact information were exposed.
* **Security Flaw:** The breach occurred due to the lack of Multi-Factor Authentication (MFA) after a server upgrade.
* **Human Error:** The security failure was caused by an overlooked basic security measure.
* **MFA Importance:** The breach shows how essential MFA is to prevent unauthorized access.
* **Attack Surface Monitoring:** A proactive monitoring solution could have detected overlooked vulnerabilities.

Learned that AI detection plays a much bigger role in cybersecurity. Just as cyberattackers can use AI to execute attacks, it can also be used by financial industries to predict vulnerabilities, strengthen authentication, and automate security measures like patching are critical techniques for improving cybersecurity in the finance sector.