T mobile

|  |  |  |
| --- | --- | --- |
| Problem: Inadequate security protocols allowed a hacker to gain unauthorized access to sensitive personal data of over 50 million customers, leading to a massive data breach. This breach exposed customer information such as social security numbers, addresses, and phone numbers, and has resulted in legal action against the company  SLACK:  Problem:  Slack's new cross-organizational DM feature allowed unsolicited messages, leading to concerns about harassment and spam. Users couldn't block unwanted invites without also blocking important ones, causing frustration. | Solution: they must establish real-time breach detection protocols and offer comprehensive identity protection services for affected customers. they must invest in security of the company.  Solution:  implement stricter controls, allowing users to accept or reject invites without receiving unsolicited messages. They should also enable granular email filtering to block unwanted invites while still allowing important communications. | Causes:  The breach was caused by weak security measures, including an unprotected router and insufficient encryption. Additionally, T-Mobile lacked real-time breach detection and regular security audits to prevent unauthorized access.  Causes:  The feature allowed users to send unsolicited messages without invitation acceptance, leading to potential abuse and harassment. Additionally, users couldn't block unwanted invites without blocking all communication from the same email address. |
| TIKTOK  Prolem:  TikTok experienced a glitch that caused incorrect follower counts and blocked user accounts, leading to widespread frustration. The issue disrupted user access and damaged the platform's reliability. | TikTok should implement more rigorous software testing and quality assurance to catch bugs before deployment. Additionally, they should have a more efficient system for quickly resolving user issues and restoring account data. | TikTok should enhance its software testing procedures to prevent glitches from affecting users. Additionally, they should implement a faster recovery process to restore affected accounts and data promptly. |
| Colonial pipiepline:  Problem:  This attack disrupted nearly half of the fuel supply in the East Coast of the United States. It also caused gasoline shortages in the Southeast and a spike in fuel prices. | **Solution:** Implement multifactor authentication (MFA) and conduct regular security testing to identify vulnerabilities. | **Cause:** The attack exploited weak VPN security without MFA and a lack of proactive cybersecurity measures. |
| TESLA  **Problem:** Tesla's Full-Self Driving (FSD) software had a glitch that caused false forward collision warnings, triggering the Automatic Emergency Braking (AEB) system and leading to sudden stops, increasing the risk of rear-end collisions. | **Solution:** Tesla released a safety recall, investigated the issue, and deployed a software update to resolve the bug and prevent further issues.  4o mini | **Cause:** The bug stemmed from a communication error in the FSD 10.3 beta software that triggered false alarms. |
| GRAND THEF AUTO:  **Problem:** Grand Theft Auto: The Trilogy – The Definitive Edition was released with numerous bugs, glitches, poor graphics, and unplayable missions, leading to a negative reception from fans. | **Solution:** Rockstar Games identified the bugs and released patches to fix the problems, but the damage to the game's reputation remains. | **Cause:** Inadequate quality control, rushed development, and poor optimization caused the game's numerous issues. |