Referring to the blog article

<https://www.testdevlab.com/blog/2021/12/27/10-biggest-software-bugs-and-tech-fails-of-2021/> .

Go through each of the defect description and try to analyse the impact (either Financial Loss, Customer Trust, Usability, User Dissatisfaction ,Security Breach etc ) and fill the following table with your findings.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Description | Impact Analysis | | | | | Solution |
| Financial Loss | Customer trust | Usability | Dissatisfaction | Security Breach |  |
| 1. **Hackers accessed T-Mobile’s systems** through a vulnerability in infrastructure, exploiting stolen credentials. | Yes  Data of 50M+ users compromised | Yes  leading to lawsuits | - | - | Yes-  Public backlash and loss of user confidence. | T-Mobile patched the vulnerability and offered credit monitoring services to affected customers. Law enforcement investigated the breach. |
| 2. **Slack’s New feature** Slack introduced a feature to message users outside the org, but it lacked safeguards and allowed unsolicited messages. | - | Yes  Privacy and safety concerns. | Yes  Poor design without abuse prevention; s | Yes  Immediate backlash; | - | Slack had to remove message customization in invites to prevent harassment and improve user safety |
| 3. **TikTok Glitch**  Users' follower count reset to zero, some accounts blocked. | - | Yes  Doubts on platform reliability. | - | Yes  Content creators lost visibility; | - | The issue was resolved quickly but underscored the importance of better software testing. |
| 4. **Colonial Pipeline Ransomware** Attac Fuel supply to the U.S. East Coast disrupted, leading to fuel shortages and price hikes | Yes  Ransom paid, economic fallout; | - | - | Yes  Gas shortages across several states. | Yes  Unauthorized access; | - |
| 5. **Toshiba Ransomware Attack** DarkSide group attacked Toshiba’s European units, exposing potentially sensitive data. | Yes  Recovery and containment costs; | Yes  Risk to client trust. | - | - | Yes  Breach in regional networks; | Toshiba refused to pay the ransom and pledged to improve security measures to prevent future attacks. |
| 6.  **Call of Duty: Warzone Glitch** A glitch allowed players to start matches with powerful custom loadouts, ruining competitive balance. | - | - | Yes  Unfair gameplay start; | - | Yes  Player frustration, rollback of feature. | Raven Software disabled the feature temporarily to fix the bug that allowed players to bypass game mechanics. |
| 7. **NHS COVID Pass Outage**  The NHS app and website were down for hours, affecting users' ability to travel due to inaccessible vaccination records. | - | Yes  Users questioned app reliability. | Yes  Downtime caused real-world issues; | Yes  Travel and event disruptions; | - | The outage lasted 4 hours, highlighting the risks of centralizing essential services in a single system. |
| 8 **Tesla Software Bug**  Tesla rolled out a Full-Self Driving update that triggered false collision alerts and braking issues, leading to a recall. | Yes  Recall costs and service efforts; | Yes  Safety concerns over FSD rollout. | - | - | Yes  Malfunctioning autonomous features; | Issued over-the-air (OTA) updates to fix the bug, recalled affected cars, and improved QA for autopilot and FSD feature releases. |
| 9. GTA Trilogy Remaster Bugs  Remastered GTA games were released with numerous bugs, graphical errors, and performance issues, angering fans. | Yes  Rockstar faced backlash, had to restore original versions. | - | Yes  Broken gameplay experience; | Yes  Game quality far below expectations; | - | Acknowledged bugs, released multiple patches, restored access to original classic versions, and promised ongoing improvements to the remaster. |
| 10. **Log4j Vulnerability**  zero-day exploit in the widely used Log4j library allowed remote code execution on millions of systems. | Yes  Urgent patches and monitoring across industries. | Yes  Affected countless organizations; | - | - | Yes  High-risk, widely exploitable; | Released urgent patches, issued public alerts, security teams worldwide scanned and mitigated the flaw, and emphasized use of software composition analysis tools. |