Problem Given	What was the impact	Actions to be taken
T-Mobile data was breached by a bad actor and acquired the personal data, and it was confirmed by T-Mobile itself. It accessed and collected more than 50 million users' data.	Due to that issue, the data which contained their names,dob,government identification numbers, driving license and many more private data.	The hacker itself told that T-Mobile used the unprotected routers, and he used them to gain access. So, they need to secure their security protocols and want to use the protected routers so in future they will protect their customer's data.
Slack receives a backlash due to the new feature that is everyone can send messages to anyone whether it is within their organization or outside of their organization.	Though it is a useful feature, we can send messages to anyone without their invitation. This leads to raising concerns about potential abusive messages and they couldn't prevent them from getting e-mail invites and they didn't have the option to block.	So, this issue can be prevented by adding block option to get prevent by the spammers. And talking about the message feature they want to add feature invitation request. So, people can accept the messages relevant to them.
Tik-Tok users faced a glitch that followers reset to Zero\Wrong followers. It also prevents some users from accessing their account.	It may be a silly thing for us but actually it is not. Nowadays the digital platform is growing, and many people are earning from this platform. So many are dependent on this. Due to less followers, the influencers may not receive their money.	Since it is software glitch, it can be prevented by going the software testing and make servers disaster recovery.
Colonial pipeline attacks faced a severe cyber attack occurred in 2021. It disrupted half of the fuel supply in east coast of United states and also caused a shortages of gasoline and increases of the fuel prices.	The attack was made possible due to the absence of multifactor authentication on a virtual private network account. This allowed hackers to exploit compromised credentials and gain unauthorized access to the network	The attack was enabled by the lack of multifactor authentication on a virtual private network account, which allowed hackers to use compromised credentials to breach the network

The Toshiba tech group faced a ransomware attack from the darkside hacking group, which threatened to expose customer data and demanded a ransom	The attack happened because of inadequate security measures that did not prevent unathorized access, allowing the hackers to exploit system vulnerabilities	Toshiba should strengthen its cybersecurity by implementing robust measure sysch as advanced threat detection system, security audits and employee training to recognize phising attempts and other attack vectors
Raven software had to remove a newly introduced pre match lobby loadout selection feature in call of duty warzone due to significant bugs. These issues provided some players with unfair advantages and disrupted overall gameplay	The glitches resulted from insufficient testing of the new feature, which failed to identify critical issues. These included payers spawning with customized loadouts and triggering an infinite dead silence effect	Raven software should adopt more rigorous testing protocols including extensive beta testing with diverse user gropus to identify and resolve potential issues before launching new features
England national health service experienced a four hour outage that impacted both its app and website preventing users from verifying their covid vaccination status and causing significant disruption for travelers	The outage likely caused by system overload or failure in the centralized, which was unable to handle the demand during a critical period	The NHS should consider decentralizing its systems to enhance resilience anf implement load testing and redundancy measure to ensure service continuity during period of high demand
Tesla recalled nearly 12,000 vehicles due to a glitch in its Full-Self Driving beta software that caused false forward collision warnings, leading to sudden automatic emergency braking and increased risk of rear-end collisions.	The issue start from a communication error within the 10.3 Full-Self Driving beta software, which triggered incorrect warning and applied for the unnecessary braking	Tesla should enhance its software testing and validation processes, and real-world scenario testing, to catch potential glitches before updates are rolled out, ensuring vehicle safety.
The Log4j vulnerability has exposed millions of web servers to potential exploitation by hackers, posing a severe threat to organizations worldwide	The issue stems from a vulnerability in the log4j logging library, which allows attackers to execute code by manipulating log messages.	Organizations should test internally to avoid defects. It should immediately make the patch to rectify the issue.

due to its widespread use in critical systems.		
Grand Theft Auto – The Definitive is have several bugs and graphics of the npc is very terrible	The old game is remake of graphic but it have several of the bugs.	It should test before release of game by the internal team to avoid bugs.