The Microsoft data breach was one of the biggest cyber-attacks in U.S. history. This was a sweeping attack on Microsoft email servers which affected more than 30,000 businesses. The hackers exploited four different zero-day vulnerabilities. This allowed hackers to obtain access to certain emails from small businesses to local governments that were unauthorized. Hackers exploited coding errors which allowed them to take over certain vulnerable systems. These hackers only needed a connection to the internet and on-premises-managed systems to break into the company's email servers. Once hackers gained access, they were able to deploy malware, request access to certain data, use backdoors to gain access to systems, and take over servers. Companies assumed the requests were legit and approved, considering they came from exchange servers themselves. Microsoft eventually patched the vulnerabilities, but if the owners of these servers didn't update the systems, attackers would still be able to take control of their system errors. Since Microsoft systems weren't on the cloud, they weren't able to patch these issues immediately. Later down the line, the Biden administration accused China of the data breach. There were a lot of repercussions because of this data breach. The main one is Microsoft consumers' data being leaked. This includes the downloading of all emails from the servers, downloading of passwords and email addresses of users in Microsoft stores, adding users, adding backdoors to systems, and accessing other systems in the network. But not only that, Microsoft lost a lot of money. People were skeptical about using Microsoft considering how weak their cybersecurity was. A lot of Microsoft users stopped using Microsoft because they didn't want their information being leaked again. Some cybersecurity measures that could've been taken to mitigate consequences or prevent the incident include safeguarding

sensitive information with data loss prevention. Other measures include Detecting, monitoring, and protecting valuable information from users who aren't authorized. Another key measure is to ensure the security and integrity of your company. Analyzing the information from this data breach, Microsoft didn’t follow all these procedures. They allowed users access to their servers because they came from exchange servers, they were in. Hackers gained control of all their servers because they didn’t use proper cybersecurity procedures. Microsoft also didn’t have all their systems on cloud so they couldn't patch these vulnerabilities immediately. These were some of the crucial cybersecurity mistakes Microsoft made. This caused Microsoft to have one of the biggest data breaches in U.S history. Which caused them to lose money, and trust from their consumers.

## References


Conger, Kate, and Sheera Frenkel. “Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China.” *The New York Times*, The New York Times, 6 Mar. 2021, www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html.

“Biggest Data Breaches in US History (Updated 2024): Upguard.” *RSS*, www.upguard.com/blog/biggest-data-breaches-us.