Sony Playstation Network Breach

One major cybersecurity breach within the past 20 years, was the Playstation Network breach, where hackers gained access to the servers containing roughly 77 million users' personal and financial information, such as their credit card information, names, email addresses, and more. When Sony discovered the breach, they took down the service for 23 days to fix their security infrastructure. Possible motivations for the breach were simple financial gain either through using the credit card information of the users they gained accessed to, or selling user information to the dark web; revenge against Sony for its legal pursuit of Playstation jailbreakers and hackers at the time; or perhaps fame and challenge of breaking into a network of a high-profile company.

The tech flaws that enabled hackers to accomplish the breach consisted of; insufficient encryption allowing the hackers to access and then extract sensitive data when they got into the network; failure to segregate sensitive data that meant the data were not separated so hackers breaking in immediately could get access to all user information; a lack of intrusion detection and response time to which hackers had plenty of time to gain loads of information before getting discovered by Song, even more so before Sony could effectively do anything to stop them; and poor patch management on Sony's part which left them vulnerable to known exploits which hackers used against them. After the debacle, Sony majorly stepped up their cybersecurity, consisting of far better encryption to prevent unauthorized access; better patch management so their network is much more secure against exploits or vulnerabilities, improved network security measures featuring better firewalls, intrusion detection, and network data segmentation; and more.