The Equifax data breach in 2017 was one of the most significant cybersecurity incidents of the past 20 years. This breach exposed the personal information of more than 147 million people, including their names, birthdates, Social Security numbers, and addresses.

The hackers who perpetrated this breach were motivated by financial gain, as the stolen personal information could be sold on the dark web. Equifax's web application framework, Apache Struts, had a vulnerability that was not patched promptly, leading to the breach.

The security flaws in this breach were a result of Equifax's negligence in updating their software with the latest security patches. The Apache Struts vulnerability was identified in March 2017, and although a patch was available, Equifax failed to patch their systems until several months later. As a result, the hackers exploited the vulnerability and gained access to sensitive data for months.

In response to the breach, Equifax has taken several measures to prevent similar vulnerabilities. They have implemented stronger cybersecurity protocols, including regular patch management, increased network segmentation, and improved encryption. They have also invested in advanced threat detection and response capabilities, utilizing artificial intelligence and machine learning to identify potential threats.

Equifax has also prioritized customer support and communication. They have provided free credit monitoring and identity theft protection services to those affected and established a dedicated website for breach updates and information.