# Assignment Document

Abwa Ndemafia Wilsmith  
FE/24/23423  
Cyber Security  
Creating a Timeline on Cyber Security  
  
Introduction  
  
Cybersecurity is a constantly evolving field, shaped by the ongoing battle between emerging threats and innovative defenses. Understanding the historical progression of cybersecurity is critical for appreciating the current landscape and anticipating future challenges. This assignment presents a timeline of key events and developments in cybersecurity history, highlighting significant milestones and their impact on modern security practices. The timeline will illustrate how the field has adapted and grown in response to ever-increasing cyber threats.  
  
Timeline of Cybersecurity Evolution  
  
Early Days (1960s – 1970s)  
\* 1969: ARPANET Creation: The Advanced Research Projects Agency Network (ARPANET), the precursor to the internet, marked the beginning of networked computing. Early security focused primarily on physical access control due to the isolated nature of systems (Video 8).  
\* 1971: The Creeper Virus: Bob Thomas created the Creeper virus, an experimental self-replicating program. While harmless, displaying the message "I'm the creeper: catch me if you can," it is considered the first known virus and a crucial moment that sparked conversations around digital security (Video 8).  
  
The Rise of Malware (1980s)  
\* 1983: The Term "Computer Virus" is Coined: Fred Cohen formally defines a computer virus in his research paper, describing a program that can infect other programs by modifying them to include a copy of itself (Video 8).  
\* 1986: The Brain Virus: Considered the first PC virus, the Brain virus, created by Pakistani brothers Amjad and Basit Farooq Alvi, targeted the boot sector of MS-DOS computers. This marked the beginning of widespread malware impacting personal computers (Video 8).  
\* 1988: The Morris Worm: Robert Tappan Morris created the Morris worm, which gained significant media attention as the first worm to spread across the internet, causing widespread disruption and highlighting the need for improved security measures (Video 8).  
  
Formalization of Cybersecurity (1990s)  
\* 1991: First Antivirus Software: As a response to the increasing threat of malware, the first antivirus software emerged to combat viruses (Video 8).  
\* 1995: Rise of the Internet: The internet becomes widely available for public use, resulting in a surge in cyber attacks such as phishing and other online fraud (Video 8).  
\* 1998: The Term "Cybersecurity" Emerges: The term "cybersecurity" begins to be widely used, and organizations like CERT (Computer Emergency Response Team) are established to coordinate responses to cyber incidents (Video 8).  
  
The Age of Data Breaches (2000s)  
\* 2000: The ILOVEYOU Virus: One of the most damaging viruses ever created, ILOVEYOU, spread through email, causing billions of dollars in damage worldwide, highlighting the potential for widespread damage (Video 8).  
\* 2003: SQL Slammer Worm: The SQL Slammer worm exploited a vulnerability in Microsoft SQL Server, causing widespread disruption and underscoring the importance of patching vulnerabilities (Video 8).  
\* 2004: PCI DSS Standard: The Payment Card Industry Data Security Standard (PCI DSS) was introduced to improve the security of credit card transactions and protect cardholder data (Video 1, 8).  
  
Advanced Persistent Threats (APTs) and State-Sponsored Attacks (2010s)  
\* 2010: Stuxnet Discovery: The discovery of Stuxnet, a sophisticated worm developed by the US and Israel to target Iran's nuclear facilities, marked the beginning of state-sponsored cyber warfare (Video 8).  
\* 2013: Target Data Breach: The Target data breach exposed the personal and financial information of over 40 million customers, highlighting vulnerabilities in retail security and the significant impact of data breaches on consumer trust (Video 8).  
\* 2016: DNC Email Leak: The Democratic National Committee (DNC) email leak, attributed to Russian hackers, underscored the impact of cyber attacks on national security and political processes (Video 8).  
  
Modern Cybersecurity Challenges (2020s – Present)  
\* 2020: COVID-19 Pandemic Impacts: The COVID-19 pandemic led to a significant increase in cyber attacks targeting remote workers and healthcare organizations, emphasizing the need for robust security measures in remote work environments (Video 8).  
\* 2021: Colonial Pipeline Ransomware Attack: The Colonial Pipeline ransomware attack disrupted fuel supplies in the US, demonstrating the vulnerability of critical infrastructure to cyber threats and the potential for significant real-world impact (Video 8).  
\* 2023: Rise of AI and Machine Learning: The rise of AI and machine learning presents both opportunities and challenges for cybersecurity, with AI being used to enhance security measures and develop more sophisticated cyber attacks (Video 8). The NIST cybersecurity framework highlights the need to identify, protect, detect, respond and recover as key functions in cyber security (Video 2).  
  
Conclusion  
  
The cybersecurity landscape has undergone a dramatic transformation from simple, relatively harmless programs to sophisticated, state-sponsored attacks with potentially devastating consequences. Each milestone in this timeline illustrates a critical lesson learned and the adaptive nature of cybersecurity professionals and technologies. As technology continues to evolve, cybersecurity must also evolve to address emerging threats and protect individuals, organizations, and nations from the ever-growing risks of the digital age. Adhering to regulatory standards, such as PCI DSS, HIPAA, SOX and GDPR is vital to ensure data privacy and security (Video 1). Implementing strong cyber security strategies such as incident response planning, security awareness training, and penetration testing are just a few essential keys to a comprehensive cybersecurity program (Video 2, 3).