THE EVOLUTION OF
CYBERSECURITY

THE EVOLUTION OF CYBERSECURITY IS MARKED BY SIGNIFICANT EVENTS AND TECHNOLOGICAL ADVANCEMENTS THAT HAVE SHAPED THE WAY WE PROTECT DIGITAL INFORMATION TODAY. BELOW IS A TIMELINE HIGHLIGHTING KEY MILESTONES,

1971: THE CREEPER VIRUS
Event: The first known computer virus, "Creeper," was created by Bob Thomas as an experimental self-replicating program on ARPANET (Advanced Research Projects Agency Network)

1983: COMPUTER VIRUS
The term "computer virus" was coined by Fred Cohen in his research paper, describing a program that could infect other programs by modifying them to include a version of itself.

1986: BRAIN VIRUS
The Brain virus, considered the first PC virus, was created by Pakistani brothers Amjad and Basit Farooq Alvi. It targeted the boot sector of the MS-DOS computers.

1988: THE MORRIS WORM
The Morris Worm created by Robert Tappan Morris became the first worms to disrupt the internet, affecting approximately 10% of computers connected to ARPANET.

1991: FIRST ANTIVIRUS SOFTWARE
Developed to combat growing malware threats.

1995: RISE IN CYBER ATTACKS
Internet accessibility for the public led to increased phishing and hacking attempts.

1998: CYBERSECURITY BECOMES MAINSTREAM
Organizations like CERT were established to coordinate responses to cyber incidents.

2000: ILOVEYOU VIRUS
A computer worm that spread through email with the subject "ILOVEYOU," causing extensive damage worldwide.

2003: SQL SLAMMER WORM
A fast-spreading worm that exploited a vulnerability in Microsoft SQL Server, causing widespread network outages.

2004: PCI-DSS
The Payment Card Industry Data Security Standard (PCI-DSS) was introduced to improve the security of credit card transactions and protect cardholder data.

2010: STUXNET WORM
A sophisticated worm targeting industrial control systems, specifically Iran's nuclear facilities.

2013: TARGET DATA BREACH
A massive data breach compromising 40 million credit and debit card accounts during the holiday shopping season.

2017: WANNACRY RANSOMWARE ATTACK
A global ransomware attack that affected over 200,000 computers across 150 countries, exploiting a vulnerability in Windows.

2018: IMPLEMENTATION OF GDPR
The European Union's General Data Protection Regulation (GDPR) came into effect, enforcing strict data protection and privacy laws.

2020: SOLARWINDS SUPPLY CHAIN ATTACK
A sophisticated cyber attack where hackers compromised SolarWinds' software updates, affecting numerous government and private organizations.

2021: COLONIAL PIPELINE RANSOMWARE ATTACK
A ransomware attack on Colonial Pipeline led to fuel supply disruptions across the U.S. East Coast.

2023: RISE OF AI-POWERED CYBER THREATS
Cybercriminals began leveraging artificial intelligence to conduct more sophisticated and targeted attacks necessitating and AI-driven cybersecurity solutions