**NAME- SEIGHA TUKOROA, 3MTT-COHORT3 - Evolution of Cyber security Milestone.**

The evolution of cybersecurity has gone through key milestones, es. Below is a summary of key cybersecurity evolution milestones.

1. **(1960s – 1970s) The Birth of Cybersecurity -** Key Takeaway: Cybersecurity emerged as a response to early vulnerabilities in computer networks, like ARPANET, demonstrated vulnerabilities.

Lesson Learned: Security was initially an afterthought, but the need for proactive measures became evident as computers began to connect. Impact: Led to the development of the first access control measures, user authentication, and early encryption methods.

1. **(1970s-1971) The emergence of computer virus Creeper -** First Computer Virus (Creeper)“Catch me if you can!” – It was created as an experiment, displaying this message on infected machines. It did not cause harm but raised awareness about network security.
2. **(1980s – Early 1990s) The Rise of Computer Viruses & Worms-** Basic password protection and physical security. One of the first major worms, it infected 10% of the internet, highlighting vulnerabilities in network security. Lesson Learned: Preventive security measures (antivirus software, firewalls) became necessary to combat malicious programs. Impact: Led to the creation of antivirus software, intrusion detection systems (IDS), and improved network security protocols.

4. **(Mid-1990s – Early 2000s) The Internet Boom and Rise of Hacking -**Key Takeaway: The commercialization of the internet increased cyber threats, including DDoS attacks, hacking groups (e.g.Yahoo, Target, Equifa, Anonymous), and large-scale breaches. Lesson Learned: Stronger authentication methods, intrusion detection systems, and ethical hacking emerged as countermeasures, and laws are needed to combat cyber crime.

5.**(2010s – 2019)Cloud Computing, Ransomware & Advanced Persistent Threats (APTs)**

Key Takeaway: The shift to cloud computing and mobile devices introduced new vulnerabilities. Lesson Learned: Security strategies had to evolve to include encryption, multi-factor authentication (MFA), and Zero Trust frameworks.

1. **(2020s Present) The Future – Quantum Computing and Next-Gen Security, AI and Machine Learning in Cyber security**

Key Takeaway: The rise of artificial intelligence (AI), machine learning, and Zero Trust security models are reshaping cyber security defense mechanisms.Lesson Learned: Traditional security approaches are no longer enough—adaptive, AI-driven threat detection and Zero Trust models are essential.

Conclusion

Cyber security has evolved from simple access control measures to AI-driven security strategies. Each milestone has reinforced the importance of proactive security measures, continuous monitoring, and strong regulations. The future of cyber security will likely focus on automation, quantum-resistant encryption, and real-time threat intelligence.