**Evolution of Cybersecurity**

Cybersecurity has been around almost as long as there have been computers. While the word cybersecurity is said to have entered the English lexicon in **1989**, cybersecurity began developing as early as the **1970s**.

Cybersecurity is growing along with the technologies that fuel the digital world. The increasing connectivity is creating new threat vectors and advancing cyber risk in business. As organizations look for ways to secure their digital environments, cybercriminals are in quest to find ways to breach these defenses. Cybersecurity has been around almost as long as there have been computers. While the word cybersecurity is said to have entered the English lexicon in **1989**, cybersecurity began developing as early as the **1970s.**

The first computer virus was created by engineer Bob Thomas. In 1971, he wrote the code for a virus called **Creeper** that could move across a network and between computers, leaving the message “I’m the creeper: Catch me if you can.”

In response to this, Ray Tomlinson (known as the inventor of email) wrote a code that searched networks to find and remove Creeper, acting as the first anti-virus program. Thus began the evolution of cyberattacks and cybersecurity.

**1980s**

The first “real” malware emerged during 1980s. While the **Morris Worm** was originally written to map the size of the internet, this computer program had the unintentional effect of slowing computers and clogging networks as it kept replicating. The code even crashed some systems altogether. To fight these cybersecurity threats and protect the increasing number of devices connected to the internet, commercial antivirus programs were developed and made their debut in **1987**.

**1990s**

The 1990s were plagued with viruses such as the **Melissa Virus**, which infected computers, overloading email servers, disrupting email accounts and slowing internet traffic to a crawl in some locations. The collective damage resulting from this virus was an estimated $80 million for the cleanup and repair of affected computer systems.

As this 1990s rolled on, antivirus software continued to evolve to identify and protect against malicious programs. A new generation of firewalls also emerged, offering a set of simple rules that controlled outside access to internal company resources.

**2000s**

The massive amount of data that became digitized in this decade created opportunities for cybercriminals and elevated risks for enterprises. This decade saw new and more sophisticated hacks that victimized government entities and well-known businesses. Massive denial-of-services attacks architected by a 15year boy took down the websites of eBay, Yahoo, Amazon and more.

At the end of the decade, cybersecurity became a major concern for both government agencies and large corporations.

**2010s**

In the 2010s, the scale of attacks increased, going beyond the intentional destruction or modification of digital assets. Over the course of the decade, credit card breaches and ransomware became more common as bad actors focused on making money from cybercrime.

As threats of data breaches and ransomware attacks increased along with the risk of these attacks leading to business disruption, loss of customer loyalty, lawsuits and regulatory fines, improving cybersecurity vaulted up the list of business priorities.

**2020–Present**

The start of this decade became known for a massive enterprise shift to remote work to keep employees safe. The surge in remote working had the knock-on effect of increasing the attack surface in enterprises, adding another potential entry point for threat actors and resulting in escalated cyber threats like ransomware, malware and phishing.

***TAKEAWAYS FOR CYBERSECURITY PRACTICES***

* Assume no network is safe, verify every user and device
* Use AI driven security tools for threat detection and incident response
* Educate users to prevent phishing and social engineering
* Employ firewalls, endpoint protection, intrusion detection, and encryption
* Follow CCPA, and Cybersecurity frameworks like NIST, ISO 2700. Cyber security practices have evolved from basic protection to AI-powered, protective, and intelligence- driven security frameworks

***A PAGE VISUAL REPRESENTATION OF THE TIMELINE ON EVOLUTION CYBERSECURITY***

A group of colorful circles with arrows

AI-generated content may be incorrect.