Key Takeaways Highlighted below:

|  |  |  |
| --- | --- | --- |
| S/N | Date | Impacts |
| 1. | Morris Worm (1988) | Led to the development of antivirus software and increased awareness about cybersecurity. |
| 2. | Melissa Virus (1999) | Improved email filtering and antivirus software, and increased awareness about email security. |
| 3. | I Love You Virus (2000) | Highlighted the need for user education and awareness programs to prevent similar attacks. |
| 4. | Stuxnet (2010) | Increased focus on industrial control system security, and development of more robust security measures for critical infrastructure. |
| 5. | Yahoo Data Breach (2013) | Led to improved password security practices, increased adoption of two-factor authentication, and stricter breach notification laws. |
| 6. | WannaCry Ransomware (2017) | Highlighted the need for regular software updates, patch management, and vulnerability scanning to prevent similar attacks. |
| 7. | NotPetya Ransomware (2017) | Increased awareness about the potential consequences of cyberattacks, and improved cybersecurity measures in global supply chains. |
| 8. | Equifax Data Breach (2017) | Led to improved data security practices, stricter breach notification laws, and increased consumer protection measures. |
| 9. | Marriott International Data Breach (2018) | Highlighted the need for improved data security practices in the hospitality industry, and increased consumer protection measures. |
| 10. | SolarWinds Cyberattack (2020) | Increased awareness about the potential for supply chain attacks, and improved cybersecurity measures in the software development lifecycle. |