WannaCry Ransomware:

Cause of Attack:
- The WannaCry ransomware attack occurred in May 2017, spreading rapidly across numerous computer networks worldwide.

Vulnerability Exploited:
- It exploited the EternalBlue vulnerability in Microsoft Windows' Server Message Block (SMB) protocol, which was a security flaw leaked by the Shadow Brokers group.

Ransomware Group:
- The attack is widely believed to be carried out by the Lazarus Group, a hacking group with ties to North Korea.

Impact:
- WannaCry affected over 230,000 computers in 150 countries.
- Major disruptions were seen in organisations like the UK's National Health Service (NHS), Spain's Telefónica, and FedEx.
- The ransomware demanded Bitcoin payments for the decryption of files.

Solutions Implemented:
- Microsoft released a critical security patch (MS17-010) in March 2017, before the attack. Post-attack, they also issued patches for unsupported versions of Windows.
- Organizations were urged to apply these patches, update their systems, and use robust antivirus solutions.
- Backup strategies and educating users about phishing attacks were emphasised to prevent future incidents.

NotPetya Ransomware:

Cause of Attack:
- NotPetya, initially appearing in June 2017, was similar to ransomware but primarily aimed at causing destruction rather than financial gain.

Vulnerability Exploited:
- It also exploited the EternalBlue vulnerability, along with another Windows vulnerability (CVE-2017-0199) for lateral movement within networks.

Ransomware Group:
- The attack is believed to be perpetrated by a group with ties to the Russian military, specifically the Sandworm group.

Impact:
- NotPetya severely affected many organisations, including Maersk, Merck, and the Ukrainian government, causing billions in damages.
- It encrypted the Master Boot Record (MBR), rendering systems inoperable.

Solutions Implemented:

- Similar to WannaCry, applying patches for EternalBlue and related vulnerabilities was crucial.
- Enhanced network segmentation and the use of updated antivirus software were recommended.
- Regular backups and incident response plans were key to mitigating damage from such attacks.

SolarWinds Cyber Attack

Cause of Attack:
The SolarWinds attack involved the insertion of malicious code into SolarWinds' Orion software updates, which were then distributed to thousands of customers, including government agencies and large corporations. The attack was sophisticated, leveraging a supply chain vulnerability to access numerous networks.

Vulnerability Exploited:
Attackers exploited the software update mechanism of SolarWinds' Orion platform, embedding a backdoor known as SUNBURST into legitimate updates.

Ransomware Group:
The attack is widely attributed to a state-sponsored group known as APT29 or Cozy Bear, linked to the Russian government.

Impact of the Attack:
The breach had widespread implications, affecting numerous U.S. government agencies, including the Treasury and Commerce Departments, and private sector companies. The attackers potentially accessed sensitive data and communications.

Solution and Remediation:
- Immediate disconnection of affected systems and networks.
- Deployment of patches and security updates to remove the backdoor.
- Comprehensive forensic investigations to understand the extent of the breach.
- Strengthening supply chain security protocols.

Change Healthcare Cyber Attack

Cause of Attack:
In early 2024, Change Healthcare experienced a significant ransomware attack that targeted its IT infrastructure, disrupting services and leading to data theft.

Vulnerability Exploited:
The attackers likely exploited unpatched vulnerabilities within Change Healthcare's systems, though specific details of the vulnerabilities remain undisclosed. bbh

Ransomware Group:
The attack was attributed to a ransomware group known for targeting healthcare organisations, but the specific group has not been publicly named.

Impact of the Attack:
The attack caused operational disruptions, delaying services and potentially compromising patient data. Change Healthcare had to halt certain services and notify affected clients.

Solution and Remediation:
- Immediate shutdown of affected systems to contain the breach.
- Deployment of incident response teams to restore services.
- Collaboration with cybersecurity firms and law enforcement.
- Strengthening of cybersecurity measures, including regular security audits and employee training.

Synnovis Cyber Attack

Cause of Attack:
In June 2024, Synnovis, a pathology partnership in London, was hit by a ransomware attack that significantly impacted its IT infrastructure and service delivery.

Vulnerability Exploited:
Specific vulnerabilities exploited have not been detailed, but the attack led to the compromise of Synnovis' administrative working drive.

Ransomware Group:
A cybercriminal group claimed responsibility, later publishing stolen data online. The name of the ransomware group is the Krillin Ransomware group.

Impact of the Attack:
The attack affected pathology services at multiple NHS trusts and primary care services in South East London, leading to significant disruptions. Over 800 planned operations and 700 outpatient appointments were rescheduled due to the attack.

Solution and Remediation:
- Implementation of manual processes for critical operations.
- Deployment of new middleware to restore IT systems incrementally.
- Collaboration with the National Cyber Security Centre (NCSC) and NHS cyber operations.
- Investigation and analysis of the published data to assess the impact.