CS405  
Merrik Wright

In November 2014, Sony Pictures Entertainment became the target of a devastating cyberattack attributed to a group calling themselves the "Guardians of Peace" (GOP). The attackers infiltrated Sony’s internal network, stole over 100 terabytes of data, released personal information on thousands of employees, and leaked unreleased films. This breach captured global attention due to its alleged ties to North Korea and political motivations related to the film The Interview, which depicted a fictional assassination of Kim Jong-un.

The attack itself combined multiple threat vectors. It began with stolen credentials and likely phishing or malware, allowing initial access. From there, the hackers moved laterally through the network, installed destructive malware, and exfiltrated massive amounts of data. Sony was a target not just for its weak internal defenses but also because of geopolitical controversy surrounding The Interview. Immediate threats included loss of sensitive data and operational disruption, while potential ongoing threats included reputational damage, blackmail, and long-term espionage.

A better implementation of layered security could have prevented or mitigated the breach. Developers should have applied the principle of least privilege, strong authentication for internal systems, better endpoint monitoring, and network segmentation. Policies addressing patch management, employee training, and intrusion detection would have strengthened Sony’s perimeter and internal defenses. SOC operations should have detected anomalous behavior sooner, especially large data exfiltration.

Authentication, Authorization, and Accounting (AAA) were all compromised. Authentication controls failed to prevent credential misuse. Authorization was too permissive, allowing lateral movement. Accounting (logging and monitoring) was inadequate, delaying detection. A stronger defense-in-depth approach—employing endpoint, host, network, and cloud security controls—could have slowed or stopped the attack at various layers, as illustrated in the diagram you shared. Governance and patch management failures were also major contributors.

In conclusion, the Sony hack exemplifies how the absence of layered, coordinated defenses and weak AAA controls can lead to catastrophic breaches. Organizations must implement defense-in-depth strategies, with strong governance, continuous monitoring, employee training, and active threat detection. Even politically motivated attacks can be thwarted or minimized with robust cybersecurity postures grounded in best practices like the NIST CSF and visual frameworks such as the one provided above.