Sony Cyber Attack Case Study

Name: Janhvi Prajapati

# 1. Lessons Learned

* • Robust, multi-layered cybersecurity defenses are essential.
* • Comprehensive incident response plans must be in place.
* • Employees should be trained to recognize cyber threats, especially phishing attempts.
* • Sensitive data and intellectual property need strong protection mechanisms.
* • Organizations should be aware of state-sponsored cyber threats and their geopolitical motives.

# 2. Recommendations

* • Implement regular cybersecurity audits and vulnerability assessments.
* • Adopt Zero Trust Architecture to minimize access-based risks.
* • Use endpoint detection and response (EDR) solutions for real-time threat monitoring.
* • Encrypt all sensitive and classified data.
* • Regularly back up data and test disaster recovery systems.
* • Engage with ethical hackers for periodic penetration testing.

# 3. Conclusion

The 2014 cyberattack on Sony Pictures Entertainment highlights the real-world dangers of cyber warfare. It not only caused financial and reputational damage but also demonstrated how geopolitical tensions can play out in cyberspace. This case is a critical reminder of the importance of being proactive about cybersecurity. By learning from such incidents and implementing robust preventive strategies, organizations can better safeguard their digital assets and maintain business continuity.