To: Prof. Kirkpatrick
From: Travon Cleveland
Bashir Bakhit
Nevin Zotaj
Date: 10/2/2015
Subject: Report on the Sony Pictures Hack 2014

The 2014 Sony Pictures hack carried out by a North Korean sponsored actors exposed sensitive data, corrupted systems, and shut down operations. It impacted all three CIA triad elements; confidentiality, integrity, and availability and caused millions in damages.

How They Did It

In late November 2014 Sony Pictures Entertainment (SPE) suffered a high-impact intrusion carried out by a group identifying as the “Guardians of Peace.” Attackers maintained access for an extended period (≈12 months), exfiltrated terabytes of sensitive data (including salaries, unreleased films and screenplays, and personally identifiable information), then deployed destructive wiper malware that erased or corrupted large portions of SPE’s infrastructure. The incident produced severe confidentiality, integrity, and availability impacts, major business disruption, and large financial and reputational costs. The attack was publicly attributed to actors tied to North Korea and included explicit political demands relating to the film The Interview.

How the CIA triad was affected

Below is a business-focused breakdown of the primary effects to each CIA leg and why they matter.

Confidentiality: Mass exfiltration of confidential material (salaries, PII, unreleased IP, internal communications).

Integrity: Attackers tampered with and corrupted system and data files (wiper overwrites, modified business documents).

Availability: Wiper malware and disrupted infrastructure caused prolonged outages across production and corporate systems.

Closing

The 2014 Sony Pictures attack is a high-value case study: it demonstrates how a state actor combined long dwell, mass exfiltration, and destructive malware to inflict technical and business damage.