

**COMSATS University, Islamabad**

**Assignment # 2**

**Case Study of a Famous Cybersecurity Scam**

**Author: Muhammad Mujtaba**

**SP22-BSE-036 1A**

**Course: ICT (CSC-101)**

**Instructor: Mam Hufsa Mohsin**

**Date: April 7, 2022**

**Abstract**

Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. Hacking might not always be for malicious purposes. It might be motivated by financial gain, protest and information gathering (spying).

In this assignment, I am going to discuss in detail, the **Sony Pictures Hack/Scam**. It was a scam by a group of hackers called “Guardians of Peace”. They hacked film company **Sony Pictures** and leaked 100 terabytes of data as well as loss of 80 million euros.



Figure : The headquarters of Sony Pictures.

**Sony Pictures Hack/Scam**

1. Introduction

November 24, 2014, a hacker group identifying itself as "**Guardians of Peace**” leaked a release of confidential data from the film studio**Sony Pictures**. The data included personal information about Sony Pictures employees and their families, emails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, plans for future Sony films, scripts for certain films, and other information. The perpetrators then employed a variant of the Shamoon wiper malware to erase Sony's computer infrastructure.

1. Objectives

The main objective of this attack was to prevent the release of the then-upcoming film ***The Interview***, a comedy about a plot to assassinate North Korean leader Kim Jong Un. The group also threatened terrorist attacks at cinemas screening the film.

1. Domain

The attack was on company named **Sony Pictures**, a film production (entertainment) company. The target users were the company’s employees and executives.

1. Technology

The attack was conducted using **malware**. Although Sony was not specifically mentioned in its advisory, US-CERT said that attackers used a**Server Message Block (SMB) Worm Tool** to conduct attacks against a major entertainment company. Components of the attack included a listening implant, backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool. The components clearly suggest an intent to gain repeated entry, extract information, and be destructive, as well as remove evidence of the attack.

1. Resolution

Sony quickly organized internal teams to try to manage the loss of data to the Internet, and contacted the **FBI** and the private security firm **FireEye** to help protect Sony employees whose personal data was exposed by the hack, repair the damaged computer infrastructure and trace the source of the leak The first public report concerning a North Korean link to the attack was published by ***Re/code*** on November 28 and later confirmed by **NBC** **News**.

1. Potential Losses

This hack caused leak of **personal** **data** of company employees and their families. It also caused loss of almost **80** **million** **euros**. In addition, the information of **then**-**unreleased** of **films** were also leaked.

In its first quarter financials for 2015, Sony Pictures set aside $15 million to deal with ongoing damages from the hack. Sony has bolstered its cyber-security infrastructure as a result, using solutions to prevent similar hacks or data loss in the future. Sony co-chairperson Amy Pascal announced in the wake of the hack that she would step down as of May 2015, and instead will become more involved with film production under Sony.

1. Lession Learnt

Sony has bolstered its cyber-security infrastructure as a result, using solutions to prevent similar hacks or data loss in the future.

Sony quickly organized internal teams to try to manage the loss of data to the Internet, and contacted the **FBI** and the private security firm **FireEye** to help protect Sony employees whose personal data was exposed by the hack, repair the damaged computer infrastructure and trace the source of the leak. The first public report concerning a North Korean link to the attack was published by ***Re/code*** on November 28 and later confirmed by **NBC** **News**.

1. Legal Responses

Obama also issued a legislative proposal to Congress to update current laws such as the Racketeer Influenced and Corrupt Organizations Act and introduce new ones to allow federal and national law enforcement officials to better respond to cybercrimes like the Sony hack, and to be able to prosecute such crimes compatibly to similar off-line crimes, while protecting the privacy of Americans.