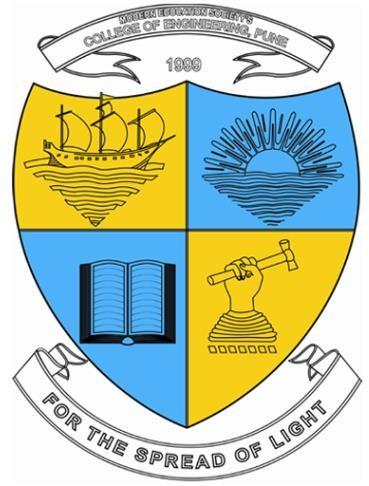
# Savitribai Phule Pune University

**Modern Education Society’s Wadia College of Engineering, Pune**

19, Bund Garden, V.K. Joag Path, Pune – 411001.

**ACCREDITED BY NAAC WITH “A++” GRADE**

**DEPARTMENT OF COMPUTER ENGINEERING**



A REPORT ON

## Cyber Crime Case Study : Investigation steps and types of evidences

## B.E. (COMP III)

*SUBMITTED BY*

Ms. Megha

**Case Study Overview: The Sony Pictures Hack (2014)**

The Sony Pictures hack in 2014 is one of the most prominent cybercrime cases in recent history. A group known as 'Guardians of Peace' (GOP) hacked Sony Pictures Entertainment's network, leaking confidential information, including unreleased films, employees' personal data, and corporate emails. The attack also included threats against the release of the movie 'The Interview.'

**Investigation Steps**

**1. Incident Detection and Response**

Detection: The hack was initially detected when employees at Sony Pictures were locked out of their computers, and a threatening message from the hackers was displayed on screens. This raised immediate alarms and led to the involvement of Sony’s IT and cybersecurity teams.

Containment: Sony's IT department quickly isolated the affected systems to prevent further spread. They disconnected critical systems from the network to avoid further damage.

**2. Initial Assessment**

Damage Assessment: The initial assessment focused on understanding the scope of the breach, identifying the compromised systems, and determining the types of data accessed or stolen. It was determined that the attackers had access to vast amounts of sensitive information.

Communication with Authorities: Sony contacted the FBI to initiate a formal investigation into the hack, providing them with initial evidence and data from their internal investigation.

**3. Forensic Investigation**

Digital Forensics: The forensic investigation team examined logs, malware samples, and network traffic to trace the attack's origin and methodology. This involved identifying the IP addresses, domains, and other technical indicators associated with the breach.

Reverse Engineering: The malware used in the attack was reverse-engineered to understand its functionality, origin, and potential ties to known hacking groups. The analysis revealed similarities with malware previously used by North Korean hackers.

**4. Attribution**

Threat Intelligence Analysis: Threat intelligence analysts compared the attack methods, tools, and infrastructure used in the Sony hack with those in previous cyber incidents. The investigation pointed towards North Korea as the likely source of the attack, supported by similar tactics used in previous attacks linked to the country.

Geopolitical Context: The release of 'The Interview,' a movie depicting a fictional assassination of North Korea's leader, provided a potential motive for the attack. This context further supported the attribution to North Korea.

**5. Legal and Regulatory Actions**

Reporting and Disclosure: Sony was required to disclose the breach to affected parties, including employees and partners, and comply with regulatory requirements regarding data breaches.

International Diplomacy: The U.S. government officially attributed the attack to North Korea, leading to diplomatic actions, including sanctions against the country.

**6. Remediation and Recovery**

System Recovery: Sony undertook a massive effort to rebuild and secure its IT infrastructure. This included implementing stronger cybersecurity measures, such as advanced threat detection systems and employee training.

Legal Proceedings: Sony faced lawsuits from employees and partners affected by the breach, which led to settlements and further legal actions.

**Types of Evidence Collected**

**1. Digital Evidence**

* Log Files: Network and system log files were crucial in tracing the attack's timeline, identifying the compromised systems, and tracking the hacker's activities within the network.
* Malware Samples: The investigation team collected and analyzed malware samples used in the attack. This evidence helped in understanding the attackers' methods and linking the hack to previous incidents.
* Network Traffic: Monitoring and analyzing network traffic provided insights into the communication between the compromised systems and the attackers' command-and-control servers.
* IP Addresses: IP addresses associated with the attack were traced back to known malicious activities linked to North Korea, aiding in the attribution process.

**2. Documentary Evidence**

* Internal Emails and Communications: Leaked internal communications were reviewed to understand the attack's impact and to identify any insider involvement or potential security lapses.
* Confidential Documents: The stolen documents, including unreleased films and corporate data, served as evidence of the breach's scope and the attackers' motives.

**3. Technical Artifacts**

* Reverse-engineered Malware: The code and behavior of the malware were analyzed, providing evidence of the techniques, tactics, and procedures (TTPs) used by the attackers.
* Forensic Images: Disk images of compromised systems were created for a detailed forensic analysis to recover deleted files and understand the attack's sequence.

**4. Threat Intelligence Reports**

* Attribution Reports: Detailed reports from threat intelligence firms and government agencies provided evidence supporting the attribution to North Korea, based on the analysis of the attackers' methods and geopolitical context.

**Conclusion**

The Sony Pictures hack case illustrates the complexity of investigating a cybercrime incident, from detecting the breach to identifying the perpetrators and securing the affected systems. The investigation relied on various types of evidence, including digital forensics, network analysis, and threat intelligence, to attribute the attack to a state-sponsored group. The case also highlighted the importance of international cooperation in addressing cyber threats and the need for robust cybersecurity measures to protect sensitive information.