

## RISK ANALYSIS /ASSESSMENT - SONY PICTURES ENTERTAINMENT DATA BREACH.

BY: **KELVIN SOLOMON PROSPER-OGUNS**

NAME OF COMPANY: **SONY PICTURES ENTERTAINMENT.**

### **STEP 1: VALUE OF INFORMATION/ASSETS:**

Aside from employee details, Sony Pictures also had in their possession new and unreleased copies of premier movies that were estimated to be about 100 Terabytes of data and in total is worth over \$8.36 Billion. The data breach was so traumatizing to staff and employees of Microsoft who had their personal identification information and that of their dependents exposed and compromised. It was recorded that employees got personal emails requesting that they stop going to work at Microsoft or face further attacks both online and physically.

Even though the technology adopted by Microsoft for Data/Assets security was not made known to the public, it is of strong belief that all data in the Microsoft possession was recreated and made redundant. The company also set aside \$15 Million to deal with the damages from the hack.

### **STEP 2: IMPORTANT ASSETS TO THE COMPANY:**

Sony Pictures as an entertainment company and at the time of the hack, did not have any reason to store more than Employee/Employee dependents details, files and copies of their released and unreleased movies/documentaries.

In this case, it is fair to say that the Assets in Sony's possession are the Personal Identification Information of employees and the Copies of Unreleased/released movies and documentaries.

It is also important to note that everything that is considered valuable should have a certain level of security depending on the value placed on it.

### **STEP 3: CYBER THREATS:**

Sony Pictures Entertainment did not specify the exact means at which the hackers used to gain access. But later reports stated that the hack was likely to occur through an employee's office computer, specifically a Malware.

It is very important to note that there are other ways the hack would have happened.

### **STEP 4: VULNERABILITIES**

The computing infrastructure used by Sony Picture's was not published, hence the limitation in looking into the weaknesses or know vulnerabilities.

But if the hack was carried out using malware, then it means it must have happened over Sony's Network.

Amongst a few, Outdated or Unpatched Software's that exposes the systems running the entire network can be a major network vulnerability that if not handled, can lead to network/service downtime. This can also lead to Distributed Denial of Service (DDOS).

### **STEP 6: IMPACT OF THE HACK ON THE COMPANY:**

As a result of the hack, Sony Picture's Co-Chairwoman Amy Pascal resigned her position due to leaked email conversations containing racist statements against then President Barack Obama. This was a Major blow for Sony's reputation.

It was also recorded that some employees who kept on receiving threat messages went on to taking legal actions against Sony for not securing and safeguarding their details in its possession.

Due to the hack, it was also recorded that Sony had to lay off some staff to enable a smooth recovery process.

The unreleased scripts and copies of movies/documentary worth Billions of dollars that were lost because of the hack was also a setback for the entertainment company.