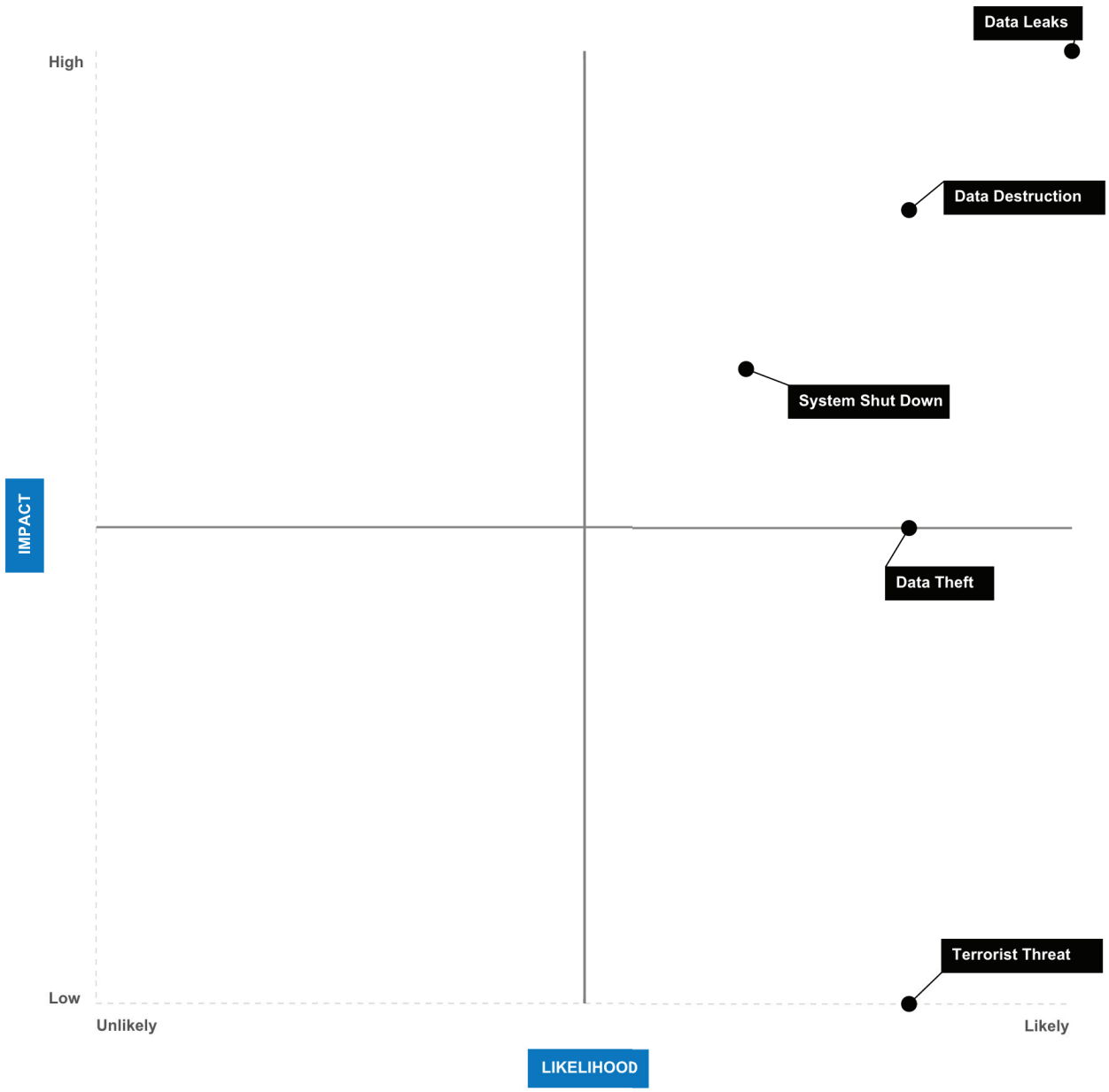

# SONY HACK EXAMPLE CASE

The following examples are based on
an individual level analysis of the 2014 Sony Hack.

Center for a New American Security

## Threat Assessment Graph



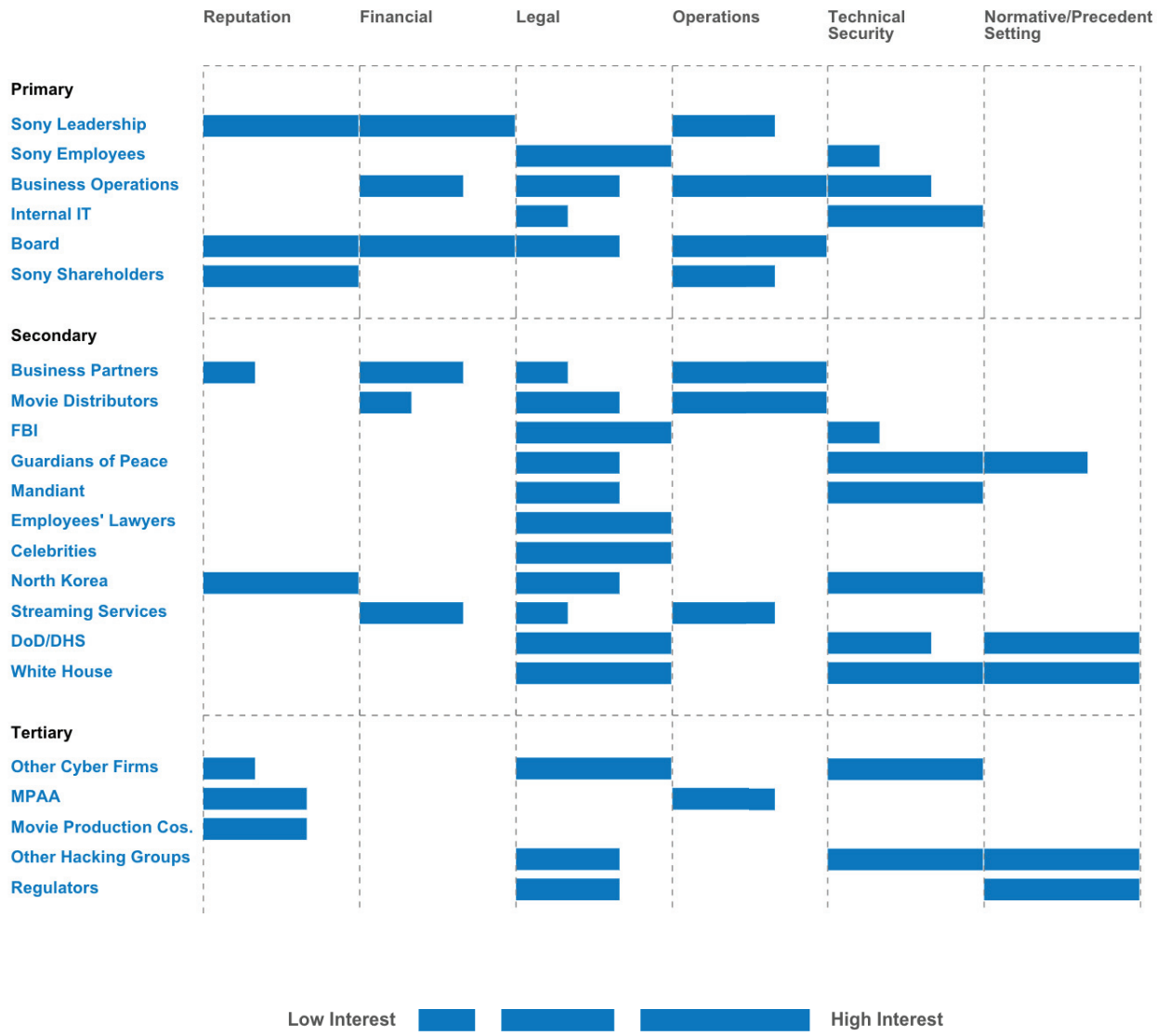

## Sample Analysis

Most of the threat objectives the Guardians of Peace (GOP) carried out against Sony Pictures Entertainment were relatively likely and high impact because of the support the GOP had from the North Korean government and the specific intent of the attack.

The terrorist threats differed somewhat from the other objectives due to the broader intent and ease with which a group can make such threats whether or not they follow through.

The data leaks and destruction were the most damaging aspects of the attack against Sony. The leaks caused significant damage to Sony's reputation while the data destruction had operational consequences.

## Issue Scoping Chart



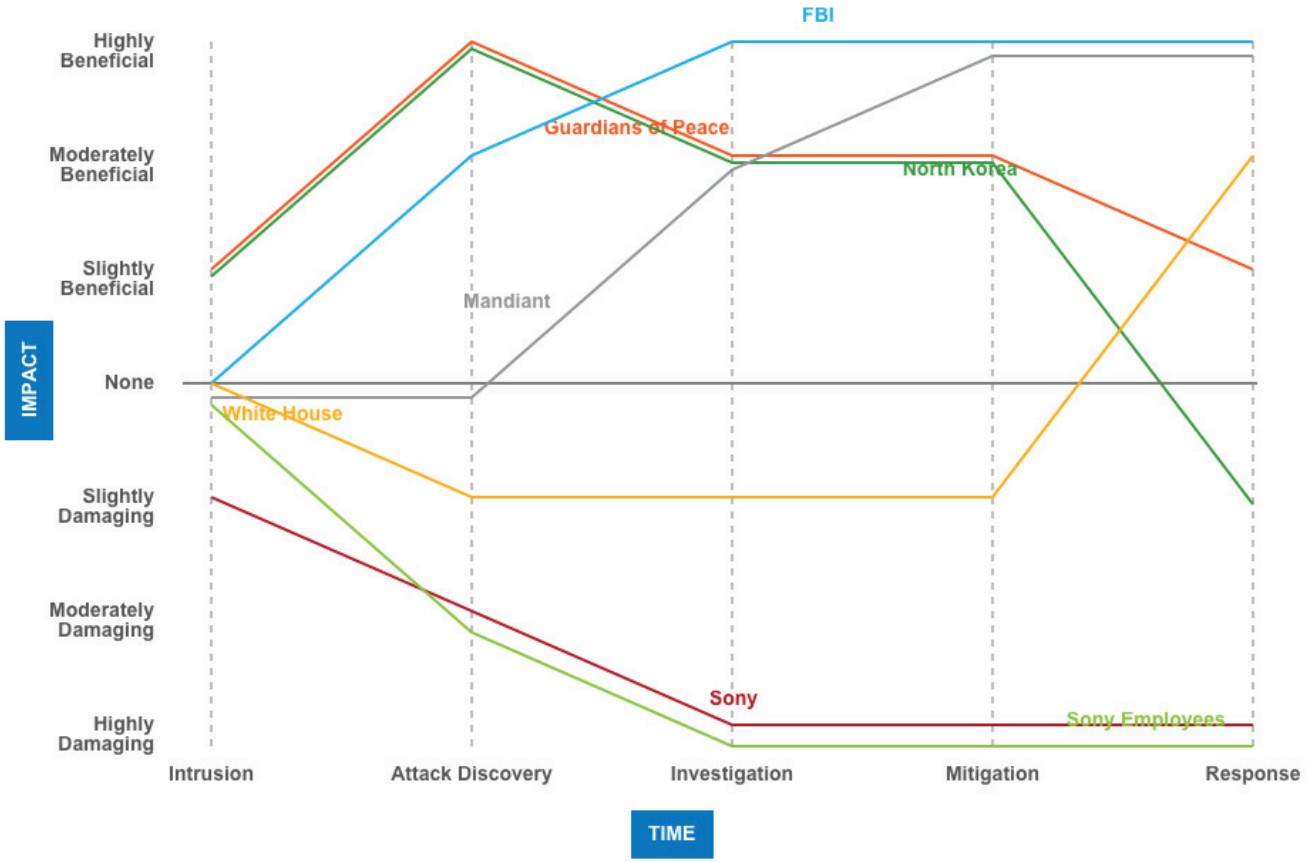

## Sample Analysis

Many stakeholders have legal interests that are not necessarily in conflict with Sony. This interest area was a prime area for Sony to foster internal partnerships to form a more coherent legal response to the attack and to cooperate with external partners such as the FBI.

While Sony leadership shares some interests with other internal groups, their financial interests clearly shaped their response to the cyber attack from the beginning, alienating them from the company and preventing the development of a more effective, holistic response.

A number of stakeholders that are more removed from the cyber attack have a broader interest in the long-term consequences of the attack on Sony insofar as they influence norms in cyberspace. Sony underestimated the importance of these interests and treated the cyber attack as an isolated incident to be solved according to internal concerns.

## Impact Over Time Graph




## Sample Analysis

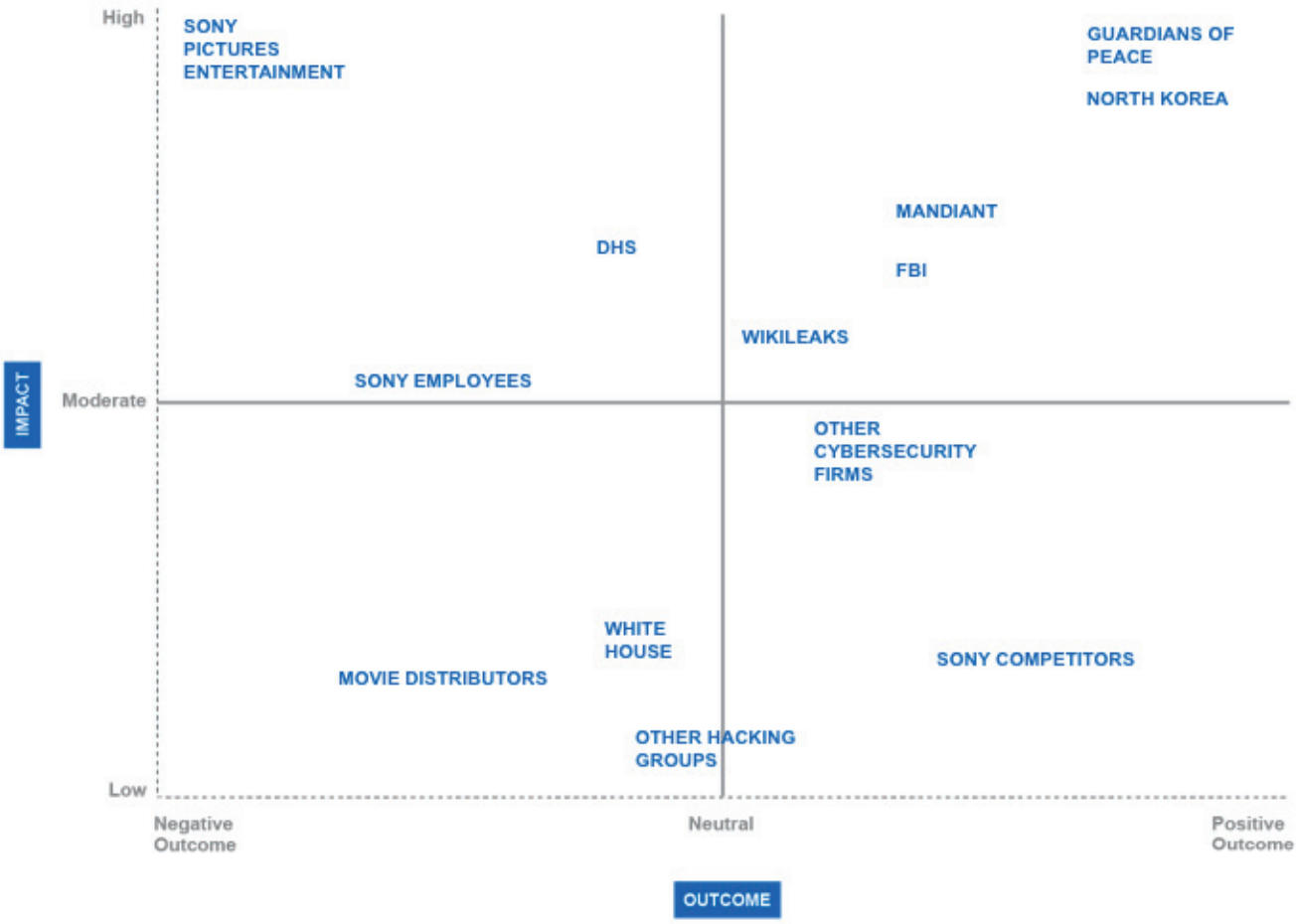
The Guardians of Peace and North Korea experienced similar outcomes up until the response phase when the United States increased sanctions against North Korean entities.

Mandiant and the FBI share similar trajectories across the phases of the Sony cyber attack because their involvement with the investigation improved their public visibility and reputations.

The White House experiences some negative impact due to the lack of coordination with Sony until the response phase when President Obama publicly critiqued Sony's response to the attack and increased sanctions against North Korean entities.

Sony and Sony employees saw continuous, worsening damage caused by Sony leadership's poor handling of the attack and the release of personal data.

## Stakeholder Map




## Sample Analysis

North Korea and the Guardians of Peace saw a high impact, positive outcome because they achieved their objective, which was witnessed by an international audience, with limited consequences.

Mandiant and the FBI experienced similar moderate impact, positive outcomes due to their high profile involvement with the investigation of the attack, which heightened interest in cybersecurity and enhanced their reputations.

While Sony employees did suffer a moderate impact, negative outcome due to the release of personal data, Sony Pictures Entertainment as a company took a harder hit because of the leadership's poor handling of the attack.

## Interest Area Scale


## Sample Analysis

North Korea and Sony both had strong reputational and economic/financial interests related to the attack but for clearly different reasons. These areas were significant drivers of action and conflict for both stakeholders.

Sony's interests were often misaligned with those of the primary U.S. government agencies responding to the attack (the FBI and DHS). Most noticeably, Sony's disregard of the political stability of U.S.-North Korea relations and national security concerns resulted in an embarrassing lack of coordination between the company and the government when crafting a response.

Civil liberties are not an important interest to the stakeholders listed on this scale and therefore played a minimal role in driving the action in response to the cyber attack.



Center for a New American Security