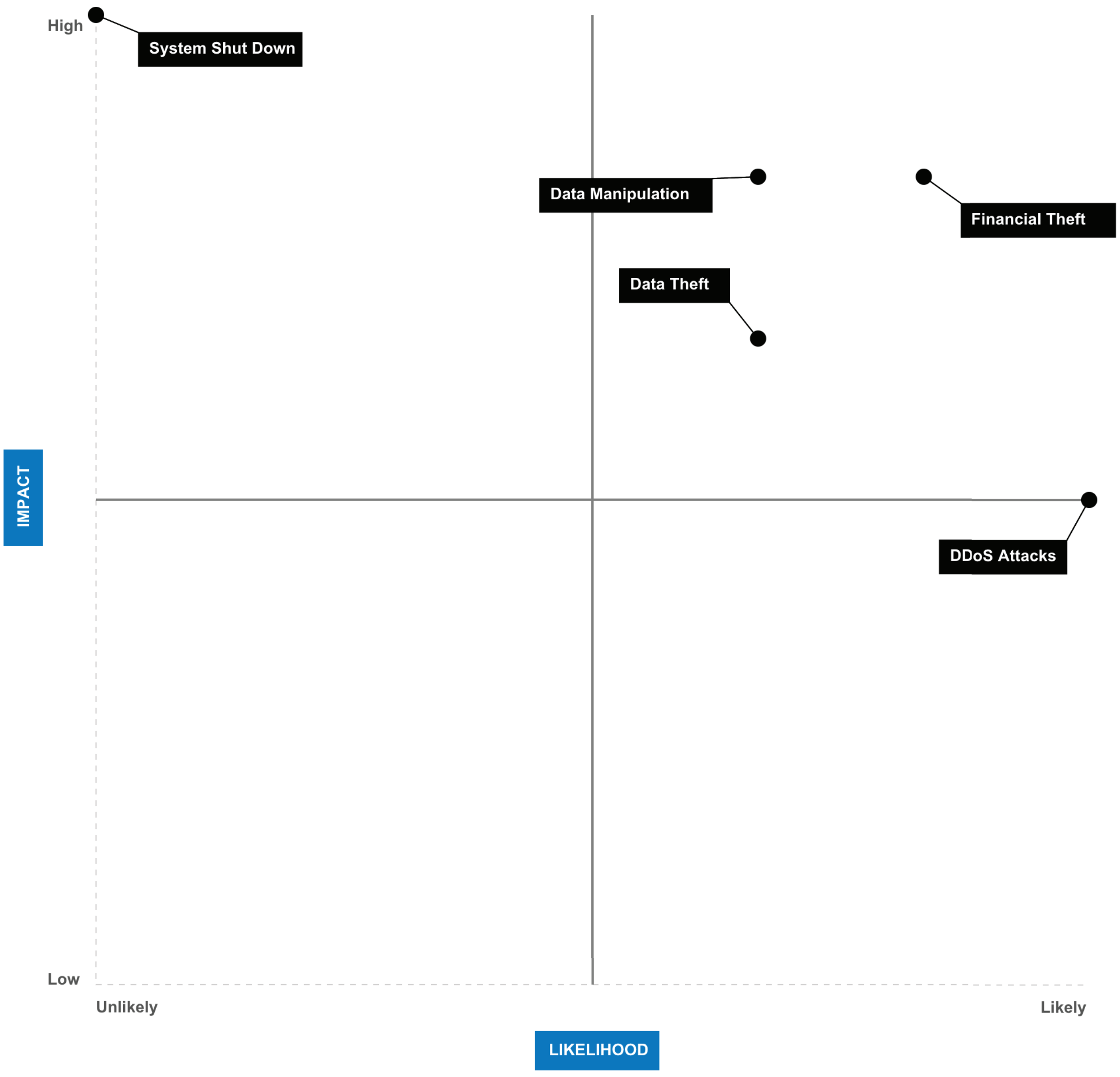
FINANCIAL SERVICES SECTOR EXAMPLE CASE

The following examples are based upon an individual level analysis of a hypothetical Financial Services Sector cyber attack:

A criminal group uses a variety of exploits to gain access to U.S.-based financial institutions' financial and customer data. The criminal group uses its access to commit fraud and sell customer data on the black market for financial gain. Financial Services Sector institutions identify the attack a few months after the initial exploit and are able to deny the criminal group's access shortly thereafter.

Threat Assessment Graph



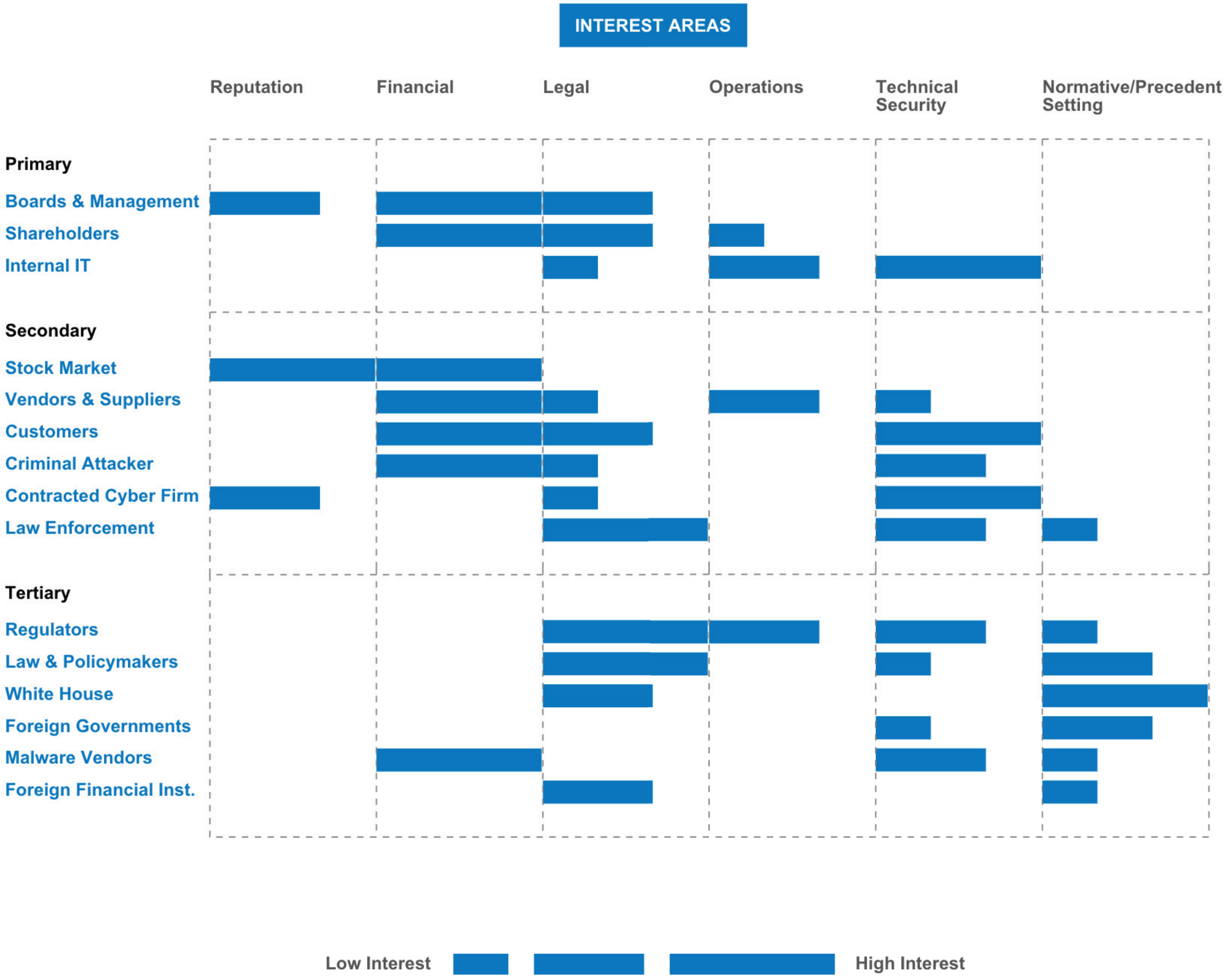
Sample Analysis

Distributed denial of service (DDoS) attacks are highly likely and relatively simple to execute with a temporary impact on operations. They are likely to be carried out by actors with political motives, such as hacktivists.

Data manipulation and theft and financial theft are similarly likely and have a relatively high impact. Attackers pursuing these aims likely have financially motivated, criminal intentions and can range from insiders to organized crime syndicates.

System shut downs are extremely unlikely due to the sophistication required to execute complete network shutdowns and the large scale economic risk posed by cascading failures. Likely attackers could include well-resourced terrorist organizations with destructive political or economic goals.

Issue Scoping Chart



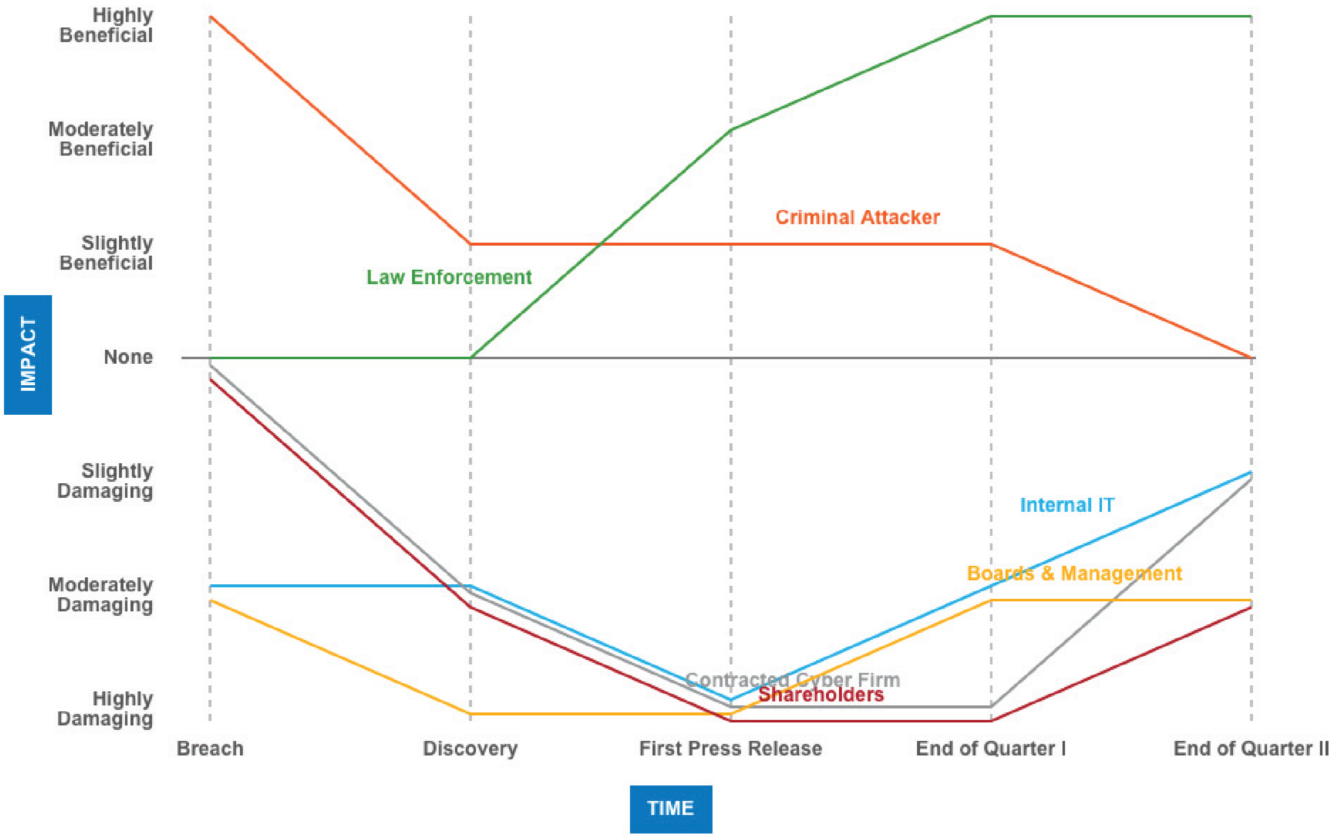
Sample Analysis

Many of the stakeholders that would be directly affected by the attack have financial, legal, and technical security interests. These are the primary areas involved in limiting the damage from and resolving the attack.

While few stakeholders are interested in operations, any preparation or incident response plans require a strategy for continuity of operations in case of a cyber attack.

Normative and precedent setting interests are held mainly by tertiary stakeholders. Directly affected stakeholders should be aware that their response to a cyber attack could shape future trends and that external groups may become involved to guide that process.

Impact Over Time Graph



Sample Analysis

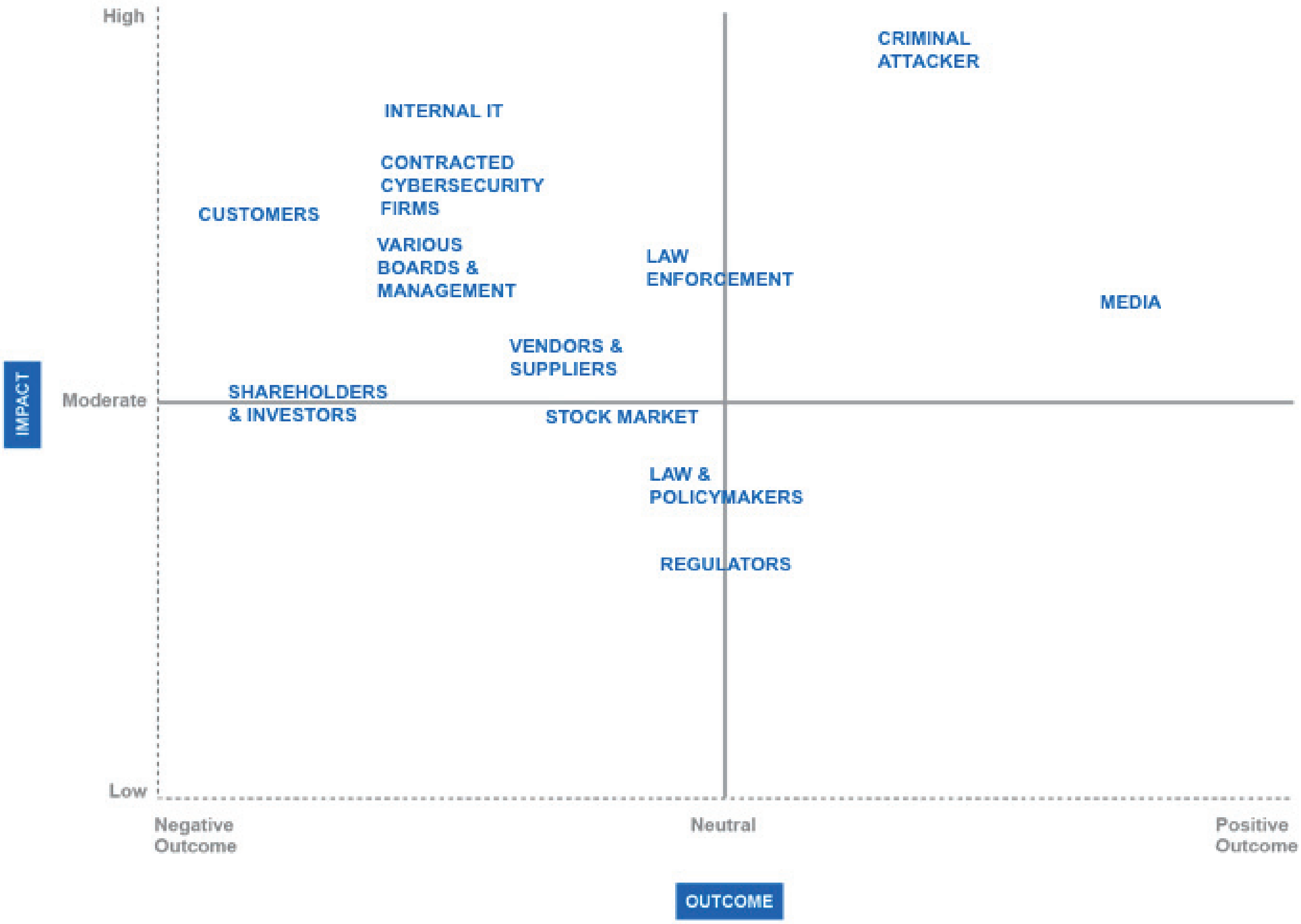
Context: After the breach is discovered, the criminal group loses access. The targeted financial institutions' reputations are damaged when the attack is publicly acknowledged and remediation costs rise. Over time, the targeted financial institutions apply the lessons learned from the attack, rendering the previous attack vectors obsolete and becoming more resilient.

Targeted financial institutions' boards, internal IT departments, shareholders, and cybersecurity providers all suffer short-term losses in the early stages of attack discovery and media coverage. The criminal attackers also lose during this stage because losing access to the financial institutions cuts them off from further financial gain.

Eventually, the defensive stakeholders recover by learning from the attack and improving cybersecurity methods. This causes further loss to the criminal attackers as it shrinks the attack surface and decreases vectors for future attacks.

Law Enforcement benefits from the media attention to cyber crime as it could support a boost to their budget, especially if the investigation results in successful attribution.

Stakeholder Map



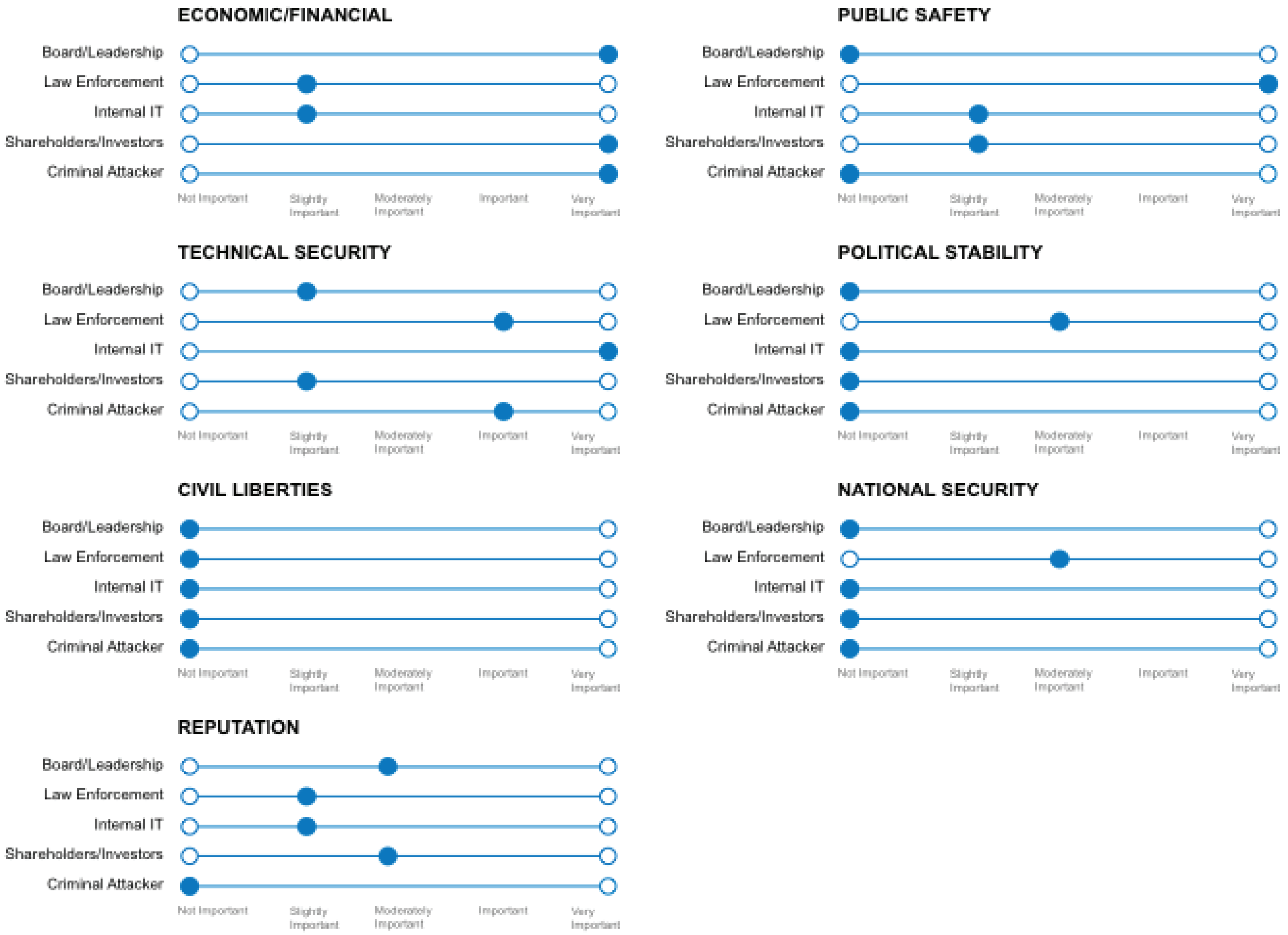
Sample Analysis

The criminal attacker experiences a high impact, positive outcome due to the financial gains they are able to make before discovery. Notably, the media also experiences a positive outcome because of a new story to attract ratings. In spite of the lack of shared interests, the criminal attacker and the media experience similar outcomes.

Law and policy makers and regulators experience a similar impact and outcome because they share an interest in managing cybersecurity practices and responses to attack.

Internal groups or actors directly associated with the targeted institutions are mapped as experiencing a relatively high impact, negative outcome. These groups are similarly invested in the continuation of profitable operations to the extent possible in case of a cyber attack.

Interest Area Scale



Center for a New American Security

Sample Analysis

Stakeholders that are part of the targeted institutions' leadership or invest in the institutions have a focused interest in institutional performance and are primarily concerned with economic/financial issues and secondly with reputation.

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

Law enforcement stakeholders have a unique set of interests compared to other stakeholders, emphasizing broader security concerns rather than the interests of targeted institutions.