Lawrencia Agyemang

IT 418

Prof. Kirkpatrick

February 21, 2022

**Report Summary**

Mergers and Acquisitions (M&A) refers to the process where one company merges with another company, during an acquisition one company buys another company. It is important to note that the specific domains present in each firm, including monetary issues, labor aspects and operational concepts, have to be integrated. The general acquirer must recognize that there are specific hazards associated with the due diligence process and that the acquiring firm is required to require certification of the assets, risks and liabilities. Depending on the current company case, the specific domains of the majority of firms are regulated and influenced in many ways by information technology, as all data, including production controllers; Decision making is done in an electronic computing environment. Therefore, cyber security is an important part of those M&A projects as governance, threats and compliance are taken into account throughout the process of due diligence, closing of deals and consolidating the entity.

It is therefore important to ensure that due diligence in the M&A process includes aspects such as performing information security analysis, identifying gaps in policy and compliance as well as prioritizing how to secure the information infrastructure of the target firm. . For example, the information systems and networks of streaming service firms undergoing M&A may be susceptible to cyber-crimes. Therefore, where there are vacancies, it is necessary to conduct a policy gap analysis to identify the inclusion of the relevant course of action. Thus cyber security

policy gap analysis should cover all security areas including data security, access control, risk detection and response as well as infrastructure security.

It goes without saying that every company should have a cyber-security policy that addresses prevention rather than cure, but it is clear that no matter what preventive measures are taken, companies can still fall victim to an attack and without a response plan, a crisis can become a disaster. However, having a plan alone is not enough for a business. Instead it should be developed, distributed, tested and modified on a regular basis. The impact of a cyber-incident can have a direct impact on the value of the business. Companies with a good track record and strong processes and procedures will generally secure more value than a business with poor records and inadequate processes.

## Cyber Security Risks

A merge does not always produce success. Sometimes mergers result in loss of value due to problems arising in search forces through technical compatibility and cyber security related risks. This often creates confusion among new management as to which employees to retain or which operations to retain. It must be well researched to make a successful merger. Considering laws in mergers and acquisition that govern and regulate data privacy, cyber risk exposure has the potential to significantly impact post-merger assessment. Unnecessary risks on the capital invested and future returns are experienced when deals are executed without cyber due diligence. Below are the two cyber risks in M&A:

### *Cyber Due Diligence Risks of the Future*

According to Controller Capital Research, 55% of the limited partners expect cyber due diligence to be done during the pre-deal. New deals tend to have more cyber analysis than the

already existing holdings. Deals made in vintages prior to 2018 are likely to be their first cyber due diligence activity in a couple of years to come, leading to cyber price erosion or showstoppers. In a period of 12-24 months, a business digital footprint is easily visible so deal teams and investors should proceed now by taking a buy-side cyber lens on their existing portfolio. Building a strong and proven cyber story bolsters the case for a stringent exit valuation.

### *Curve-out and Integration Risks*

M&A activities are the greatest incubator for deadly cyber-attacks and many businesses have discovered this after huge losses. Integration of businesses in a complex patchwork of systems with security blind spots and vulnerabilities has led to the downfall of most businesses. A hacker can go dormant for years only to be awakened in a newly integrated core business. Managers need to avoid excessive risk and assumption that the party has already reached a settlement, then carve out or set an integration strategy with a clear target operating model. Value comes first in protecting core business.

## Conclusion

Finally, a major part of any assessment of the cyber security situation and capabilities of the target should be the assessment of the personnel with that responsibility. This should not be limited to target's employees only; however, outside contractors can also be used to provide specialist expertise. Part of Target's cyber security has limited value in being available only during regular business hours. At the very least, there should be a mechanism to garner support for hours without lengthy discussions.