Reduce Risk With Better Cyber Due Diligence

MARCH 2022

by Luke Tenery and Ross Rustici

Luke Tenery
Partner, StoneTurn
ltenery@stoneturn.com
+1 312 775 1210

Ross M. Rustici
Managing Director, StoneTurn
rrustici@stoneturn.com
+1 617 570 3716

As regulators continue to propose new rules and speak publicly about expanding enforcement, the risks associated with mergers and acquisitions are on the rise. A lack of satisfactory due diligence often results in the onboarding of not only a new asset but also legacy security risks and ongoing security incidents. Not only does this result in a slower integration of assets, but it also increases the costs associated with M&A and has the potential to reduce expected gains. Additionally, this is likely to become a new avenue for regulatory enforcement as policy and technical mitigations become a larger part of the purview of regulators.

Just as in conventional due diligence, not all assets merit the same level of scrutiny. There are several considerations that go into assessing the requirements of cyber due diligence and the trade-off they impose on deals, both in terms of time to execution as well as friction with the target company or asset.

The least intrusive and easiest type of check to run is an external risk score. This kind of assessment creates a baseline of knowledge about the public exposure of a target company. Looking at data such as open ports, encryption certificates, and misconfigured cloud assets, an external scan

StoneTurn

of company resources can provide a valuable and nonintrusive understanding of how the company is currently operating.

However, this method is prone to high error rates when assessing the security posture of a company, as most of the data that can be collected by these methods can have technical mitigations that are not easily detected in these scanning techniques. Additionally, the datasets used for this type of analysis is often flawed as IP addresses and technical assets often are not updated when they change owners, resulting in scores being calculated on other company's assets.

Digging More Deeply Into Risk

The next level of diligence builds on top of the scanning capabilities and conducts research into the company, its key individuals, and existing leaked or targeting data. This activity — conducted without any direct interaction with the target company or asset — focuses on finding data that would enable exploitation of their networks or existing evidence of ongoing targeting and exploitation. Not only will this level of review uncover information that can be leveraged by hackers to gain unauthorized access in to the company's systems, but it also provides insight into the company's security culture. How often do engineers post sensitive information on tech forms when asking for assistance? How much information do employees share when helping others on similar forums? How many proprietary documents have been accidentally uploaded to VirusTotal or other sites?

This all speaks to security culture and allows for an assessment of what problems are likely to exist internally. Understanding this culture and the weak points that are already public enables more informed questions during the rest of the diligence and also can be leveraged to enable an internal security review.

The most intrusive diligence is an audit of existing controls, policies, and detections. This will give the highest level of assurance but may also cause the most friction as it requires third-party access to sensitive technical information. However, this is the best way to gain assurance around the level of risk a company is assuming during an acquisition. How secure a company currently is and if there are any indications of ongoing compromise can only be done with internal data.

Why Increase Cyber Diligence During M&A?

Findings associated with this analysis can materially affect deal size, expected returns, and integration plans. Finding problems prior to merging IT assets will provide long-term savings after a deal is concluded but could interrupt short-term goals. Having a firm grasp on what the acquirer will be faced with allows for better earnings projections and a better deal valuation overall.

Additionally, as regulators continue to focus on cybersecurity, the likelihood of increased scrutiny and potential fines is only increasing. The risk of acquiring a compromise or permitting a continued culture of disregarding security and privacy concerns during the M&A process is increasingly likely to result in regulatory action, making the new asset a potential liability before the expected returns can be realized.

As industries continue their march toward digital transformation, the security and culture around those key business assets can either undermine or reinforce their value. Cyber diligence is rapidly becoming essential. Building a sustainable and objective framework around the level of diligence will become more valuable as the private sector becomes more regulated and technology-reliant.

This article originally appeared in **Dark Reading, March 2022.** All rights reserved.

About the Authors

Luke Tenery, a Partner with StoneTurn, brings nearly 20 years of experience helping leading organizations mitigate complex cybersecurity, data privacy and data protection risks.

Ross Rustici, a Managing Director with StoneTurn, has over a decade of experience advising governments and global corporations on cybersecurity matters, as well as building security and intelligence programs for clients.