Maintaining Cybersecurity During Mergers & Acquisitions

Mergers and acquisitions are risky times. Headlines treat the combination of companies as job done after the announcement, but insiders know combining operations is no easy task.

These days, add cyber risk to the list of prime considerations companies should weigh before, during, and after any M&A decision.

Companies involved in transactions are often prime targets for hackers and cybercriminals. The high-pressure environment of a M&A can cause key players to act carelessly, leading to exploited vulnerabilities that pose risks to the deal's value and return on investment.

Actually, these days even the law firms and financial advisers that handle transactions are prime targets. The value of confidential deal-related information is high and published reports show sophisticated hackers targeting the trade secret and market-moving data held by third parties.

Directors should be aware of the risks each stage of a transaction poses and ensure management conducts a risk assessment for each phase.

In 2014, and again with a revised edition in 2017, the National Association of Corporate Directors teamed with the Internet Security Alliance to produce a handbook guiding directors in overseeing this difficult terrain.

On June 21, NACD, in partnership with ISA, hosted a full day event in Chicago that brought together directors, executives, and cybersecurity experts to share real-world insights and critical action steps for boards to foster enterprise-wide cyber resiliency. In the appendix of the Handbook is a section outlining key issues boards should consider during M&As.

Strategy and Target Identification Phase

Attackers look for hints a company is considering a merger, acquisition, or divestiture. They may be tipped off by industry gossip, staff reductions or a slowdown in a company's release cycle. The acquiring company at this stage should gain an outsiders' understanding of the cyber risk the target poses.

Management can do so by searching for signs of a past cyberattack as demonstrated by stolen intellectual property or company logon credentials for sale online. Check the status of the target's network defenses and whether they have holes. Model the financial impact of identified cyber risks, since they may result in loss of competitive advantage and complications like costly remediation or even litigation.

Companies should also consider risks posed by third parties involved in this, and future phases. Do their contracts include cybersecurity requirements? How are they enforced, do they indemnify against a cyberattack?

Unfortunately, company insiders may also pose a risk. Full time employees, contractors or vendors may release sensitive data and information, whether intentionally, through negligence, or otherwise. Insiders often pose the greatest threat and leading practices to diminish their risk require enterprise-wide collaboration by functions as diverse as human resources, legal, and compliance, as well as the IT department.

Due Diligence and Deal Execution Phases

Know what you're buying when it comes to cyber risk. Has the target company invested sufficiently in cybersecurity, including personnel? Does senior management exhibit a lax attitude toward cyber risk? Is there an insider threat program? Are there cybersecurity-related terms and conditions in supplier contracts that have financial impact or liability consequences?

Depending on the risks, the board may want to defer transaction approval until remediation is complete, have the price renegotiated or even withhold approval, should the risks prove too great.

This phase also holds the potential for increased risk since the rush toward completion may inadvertently open digital doors to attackers.

Integration Phase

Hackers can spy an advantage in a newly merged company with inconsistent platforms and technology operations. Integration teams should delve into the smallest of details to ensure that security gaps not already mitigated are filled. Employees will need training on how to securely handle newly integrated systems, too.

Post-Transaction Value Creation Phase

Management should continue to evaluate the cyber maturity of the merged entity by benchmarking against industry standards. Low maturity could impact growth projects and hurt brand reputation.

Written by Dave Perera, ISA Assistant Vice-President for Government and Policy