Kevane Grant Thornton

Advisory

Organizations

Cybersecurity

Cybersecurity in M&A strategy

October 18, 2021

Mergers and acquisitions require a mix of strategic and tactical work – cybersecurity is usually an item on the tactical list.

Many organizations are drawing up plans for mergers and acquisitions right now, as leaders look for growth after the pandemic slowdown, and as new business models emerge. However, weakened cybersecurity hygiene throughout the last year means that these M&A transactions elevate the risk of cybersecurity incidents.

Create an M&A cybersecurity playbook

As an M&A deal progresses through its lifecycle, cybersecurity and data privacy risks steadily increase.

To successfully identify and monitor these risks in an ongoing and repeatable way, companies need an M&A cybersecurity playbook.

The M&A cybersecurity playbook can be broken into four stages:

1. **screening**: during the screening stage, have a key stakeholder looking out for cybersecurity and privacy risks. Information security leaders within the firm are ideal candidates for this position. Also identify the target's information security team composition and qualifications.
2. **due diligence**: due diligence is the most important stage of the deal before day one of the transaction, and cybersecurity and privacy must be thoroughly evaluated at this stage to avoid any future regrets. Conduct cybersecurity risk assessments, vulnerability scans, penetration tests, and compromise assessment to the point agreeable. Evaluate compliance with privacy and regulatory requirements and look out for past and current findings or security and privacy incidents.
3. **announcement:** there can be a lot of media coverage during the announcement stage, which sometimes alerts malicious groups and other threats.
4. **closure**: when the deal is being completed in this final stage, the cybersecurity and privacy actions required for success are far from being complete. Cybersecurity integration in this stage can be the most challenging part of the deal journey, as the acquirer and target look to integrate capabilities across both firms.

Create an M&A cybersecurity framework

An M&A cybersecurity framework can provide a template for guiding cybersecurity integration. The framework builds upon the careful consideration given to cybersecurity and privacy matters during the due diligence stage. The findings from the due diligence results lay the foundation for the integration effort.

The cybersecurity framework should focus on four key factors, with the end in mind:

1. enable business goals
2. reduce cyber risks
3. advance cybersecurity program maturity
4. contain business-as-usual (BAU) costs

Execute the M&A cybersecurity plan

Your M&A cybersecurity execution plan needs to leverage the M&A cybersecurity playbook and framework with both tactical and strategic actions planned along the M&A journey.

Tactical actions:

- specific cybersecurity threat monitoring must begin on day one and continue for at least the first phase of the merger or acquisition.
- the due diligence risk assessment feeds into remediation of the high-risk issues, followed by remediation of the medium-risk and low-risk issues if needed.
- a compromise assessment provides important input for identifying and isolating potential incidents and taking immediate actions to address them.

Strategic actions:

- a comparative analysis of cybersecurity capabilities will inform the cybersecurity consolidation, business solution migration and subsequent support.
- the cybersecurity integration strategy forms an important foundation for integrating cybersecurity policies, processes, and suppliers.
- the target operating model for cybersecurity, once designed and established, will implement a one-team approach in supporting the cybersecurity program going forward with defined performance metrics and control monitoring.

The M&A cybersecurity playbook and framework execution must include change management to ensure that business users are on board and can continue business as usual. Throughout the M&A transaction, your project management and change enablement resources should be fully engaged. Make sure to prepare your team's skill sets, bench strength and industry expertise in advance. Evaluate and prepare any additional internal and external cybersecurity resources that you will need to call upon during the transactions.

In the crucial period before and after a merger, cybersecurity teams have a unique opportunity to reduce risks and add value to the business. However, they must employ careful planning, precise execution and close consultation with business and IT leaders to ensure a successful cybersecurity integration.

Grant Thornton library articles:
Cybersecurity in M&A strategy

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter, we will be glad to assist you.

Advisory Senior Manager
E marta.rodriguez@pr.gt.com

Neysha Otero
Advisory Manager
E neysha.otero@pr.gt.com

Jorge Paredes
Advisory Manager
E jorge.paredes@pr.gt.com

Advisory Manager
E jorge.oquendo@pr.gt.com

Kevane Grant Thornton

grantthornton.pr