VECTRA

The CISO’s M&A Risk Checklist

Track, identify, and resolve M&A risks that should be top of mind.

As the CISO, you’re the tip of the spear for identifying, managing, and eliminating risk in the M&A process. Most risk factors will fall into one of three categories:

1 People

2 Process & procedures

(applies to associated third parties as well)

3 Infrastructure

These risks are present on both sides of the M&A deal.

M&A Risk Factors

1 PEOPLE RISK FACTORS

Find out from leadership as early as possible plans for both staff after the deal closes to minimize unease and any potential damage.

Will staff be: □ **Integrated** or □ **Consolidated**

If staff will be Integrated, have leadership provide:

- □ Personnel list
- □ Integration schedule
- □ Explanation of how staff will be integrated
- □ Data access map for each employee

If staff will be Consolidated, ask leadership for:

- □ Positions that will be cut on your side and when
- □ Positions that will be cut on the other side and when
- □ Knowledge and access levels each employee possesses

Capture legacy knowledge by identifying:

- □ Key players in the target firm
- □ How these key players operate
- □ Differing operational styles, potential conflicts, and priorities
- □ Third-party connections and how they operate within the target company

2 PROCESS AND PROCEDURAL RISK FACTORS

To move the M&A process forward and minimize losses, regular routines can be disrupted and new demands can be added, making your organization vulnerable to insider threats, loss of IP control, and other security problems.

Meet with leadership to establish:

The Day-to-Day Schedule M&A Processes & Procedures for

- □ Your team
- □ Target team

What Procedural Adjustments Will Need to be Made by

- □ Your team
- □ Target team

Prioritize & Schedule of Adjustments to be Made by

- □ Your team
- □ Target team

Process for Suggesting & Implementing Process Adjustments

- □ In your team
- □ In the target team
- □ Identify how much disruption the business can take
- □ Identify who is in charge of managing the transition and disruption
- □ Synch procedures with the transition manager

Manage Confidentiality & Business Reputation Risk

- □ Identify your initial, small security team, aka your A Team
- □ Identify the earliest possible engagement of A Team with the M&A process
- □ Identify a process to silo confidential information with your A Team
- □ Identify a process to coordinate and silo confidentiality with counterparts on the target team

Manage Third-Party Risk of Vendors & Service Providers

- □ Identify all of the target team's current third-party vendors and service providers within the past 3 years
- □ Obtain each third-party consultant's procedures with the target company
- □ Coordinate with each third party to make the process go as smoothly and discreetly as possible.
- □ Identify secondary third-party vendors used by the target team's third-party vendors and service providers
  1. Managed service providers
  2. Managed security service provider (MSSP)
  3. Managed security providers for IT, etc.
- □ Manage all in a central hub (Data Room) to de-risk all third-party vendors (See Item G below)

A Data Room to Identify & Categorize Risk

- □ Define a clear methodology for data gathering and reporting
- □ Create a set of robust questions around statements of work, bills of materials, etc., so you see the normal business flow
- □ Capture all information, data, procedures, infrastructure, and supply chains of products and services
- □ Identify any dependencies of the target team
- □ Examine all third-party contracts of the target firm: Help Desk Tier 1, system engineering, infrastructure stack, supply chains of services, product dependencies, etc.
- □ Prepare robust follow-up questions for clarity, depth, and accuracy and to surface unseen vulnerabilities
- □ Identify what's working in this process. (List)
- □ Identify what's not working in this process (List)

3 WHAT RISK FACTORS DO WE INHERIT FROM THE TRANSACTION?

Unacceptable risk from either side can devalue the deal.

How can you minimize and manage risks from the company you're merging with or acquiring?

- □ **Manage bi-directional risks like flood gates, one channel risk analysis at a time**
- □ **Integrate target company channel by channel**
  - □ Identify incompatible security technology stacks
  - □ Identify and prioritize conflicting views on security best practices
  - □ Identify out-of-date SOC protocols or other factors that require time to identify, assess, and resolve

4 4. WHAT RISK FACTORS DO WE INTRODUCE INTO THE TRANSACTION?

Identify risks your company brings to the deal.

List and address each:

- □ **Are there internal practices that need to be updated to a standard?**

____

____

- □ **Is/Are there a channel(s) that lack visibility or have prior breach(es)? If yes, list them and address each**

____

____

- □ **Are all security technology stacks up to standards?**

____

____

- □ **Identify and adjust security best practices that are native only to your team**

____

____

- □ **Identify any other factors that need to be resolved before ecosystem integration**

____

____

- □ **Prioritize those systems that are critical to the business first**
- □ **Expect to adjust to some system overlap**
- □ **Unravel risk factors in Salesforce, your ERP solution, go-to-market MarTech, etc.**
- □ **Don't expect to complete the systems integration at close, but as risks are identified and mitigated**
- □ **Prepare for and accept a level of disruption**
- □ **Prepare for lower efficiency and productivity during risk assessment and mitigation processes**
- □ **Before integrating business processes, know where compliance requirements differ, i.e., the target firm processes credit cards and yours doesn't, etc.**
- □ **Reconcile all security differences and priorities with the proper stakeholders before any integration**

5 THE TOP 3 TAKEAWAYS FOR CISOS TO BE SUCCESSFUL IN THE M&A PROCESS

1. Have ownership of the "go or no go" decision

- □ Do your stakeholders understand the risks you've surfaced and why you've made the call to proceed with or cease the M&A process?
- □ Will stakeholders back you up on your assessment when you provide the evidence?

2. Navigate Trust Boundaries

- □ Establish trust boundaries between people, processes, and technologies
- □ Determine if the people you're working with are trustworthy
  - □ Identify reasons not to trust someone, if present
  - □ Identify all insider threat possibilities – if present

3. Keep Your Ears Open at All Times for "Unofficial" Information About Target Company

- □ Attend onsite and corporate functions because you may hear things that legal or the board may not, that can provide vital information about the company that you may not see in official documents

For more information on how to prepare for transitions, be sure to check out our full Vectra AI compliance guide.

About Vectra AI

Vectra® is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai