FRSECURE

FRSecure Mergers and Acquisitions Security Checklist

Mergers and Acquisitions Cybersecurity Checklist

Here are some key things that should be looked at throughout an M&A process.

Any time a company is going to acquire another organization or a portion of an organization through purchase or merger, it's critical to know what security risks might come with the acquisition. Without knowing, organizations open themselves up to significant financial and legal challenges.

By nature, mergers and acquisitions typically take place in a relatively secretive manner. Because of this, very few people are given information about the acquisition ahead of time. Still, organizations always take the time and effort to do their financial due diligence before any merger exists. Information security due diligence is often an afterthought but needs to be taken just as seriously given the potential business impact of security risks.

How security governance managed? What will the technical resources look like? What type of data does the purchased company hold? Who are their critical vendors? What are their most significant risks?

Before

As the company is looking for other organizations to acquire

- [ ] Perform a risk assessment
  - [ ] Consider size of the organization, complexity, and compliance requirements
- [ ] Understand their risk profile
  - [ ] Determine when their last comprehensive information security risk assessment was done
  - [ ] Determine who has the results of the last risk assessment
  - [ ] Determine the steps that were taken to reduce those risks
  - [ ] Recognize inherent risk
    - [ ] Search for any active breaches
    - [ ] Understand that even with your own strong security program, you inherit the risk of the new organization you acquire/merge with
- [ ] Consider legal requirements
  - [ ] Who are the company's critical vendors and what critical business operations are dependent on vendors

- [ ] Determine if the organization has paid fines or is under a current FTC consent order for security breaches
- [ ] Identify if the organization have any current security certifications or attestations (e.g., ISO27001, SOC1 or 2) to maintain
- [ ] Determine data ownership, including historical data if only a portion of the company is being acquired
- [ ] Understand if there are new laws and regulations you will have to follow
    - [ ] Based on location
    - [ ] Based on industry
    - [ ] Based on business type
    - [ ] Based on the data stored/collected

During

While merging the two organizations

- [ ] Take time to learn all the ins and outs of the new organization you're about to take control of
    - [ ] Review their incident response plan
    - [ ] Review their business continuity plan
    - [ ] Review their disaster recovery plan
    - [ ] Review the vendor management program
    - [ ] Understand what's in place so you can adequately take control of them
- [ ] Begin creating or reviewing an asset inventory
    - [ ] Physical (computers, servers, etc.)
    - [ ] Logical (data, applications)
    - [ ] Software (standard packages, licensed, supported)
    - [ ] Legacy systems
    - [ ] Code management/escrowed
    - [ ] Are managed services used - Infrastructure, Security, Monitoring, Data Center colo, etc.
- [ ] Is there a vendor management program in place, have risk assessments been performed on critical vendors?

- [ ] Determine what access controls they have in place
    - [ ] Understand if access is on a need-to-know basis or if it's looser
- [ ] Understand what the technical infrastructure looks like
    - [ ] Determine if and how you will integrate:
    - [ ] Check servers, PCs, and networks for currency and warranty
    - [ ] Create a plan for anything obsolete, out of date, and no longer supported
    - [ ] Find out what is standardized and what isn't
        - [ ] Data flow
        - [ ] Is data encrypted at rest
        - [ ] Where are backups maintain – cloud or physical location
        - [ ] System protection with up-to-date patching, end point protection, and firewalls
        - [ ] Controls for internet-connected networks
        - [ ] Adequate firewall rules
        - [ ] Systems allowed to communicate to and from the Internet
        - [ ] Connectivity with third-parties
- [ ] Check for physical security measures
    - [ ] Are facilities included and how many are involved
    - [ ] Where is the data center – on premises, at a colocation, cloud
    - [ ] Are facilities owned or leased
    - [ ] Determine if access into and out of their facility is controlled
    - [ ] Look for extra protections on critical areas (like server and network rooms)
    - [ ] Review current faculty safety controls

After

Once the transition or merge is completed

- [ ] Review and adjust governance
  - [ ] Align information security and HR policies and communicate any changes with all employees
  - [ ] Train employees so they know, understand, and follow policies
  - [ ] Get updated policy acknowledgements from all employees
- [ ] Conduct ongoing evaluations
  - [ ] Establish the new baseline for information security
  - [ ] Ensure personnel follow requirements
  - [ ] Determine which departments and security practices to spend time training
  - [ ] Get a validated risk assessment annually
    - [ ] Recognize which measures are a business priority
    - [ ] Prepare to make changes based on the results and priority
  - [ ] Update audit and compliance plans to encompass new assets
  - [ ] Update scope on certifications and attestations if impacted
  - [ ] Communicate changes with external auditors